EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JAVIER FELIPE BULLA AGUILAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERÍA DE SISTEMAS

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)

TUNJA - BOYACÁ

2019

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JAVIER FELIPE BULLA AGUILAR

Trabajo de Diplomado para optar por el título de Ingeniero De Sistemas

Director Diplomado profundización

Ing. JUAN CARLOS VESGA

Tutor Ing. DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERÍA DE SISTEMAS

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)

TUNJA -B OYACÁ

2019

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

Presidente del Jurado

Jurado

Jurado

DEDICATORIA

Dedico este trabajo con mucho amor a:

Mi Mamá Rosa, Y hermano Santiago quienes siempre me apoyaron, me tuvieron paciencia y no permitió que desistiera por más difíciles que fueran mis metas.

Esta meta no es mía es de nosotros, mamá, hermano.

Los quiero y son indispensables en mi vida.

Gracias.

Tunja – Boyacá, 12 de diciembre de 2019

AGRADECIMIENTOS

Expreso mi agradecimiento sincero al directo del Diplomado De Profundización Cisco, ING. JUAN CARLOS VESGA por su acompañamiento y atender con prontitud mis inquietudes.

Gracias a mi tutor ING. DIEGO EDINSON RAMIREZ, por siempre estar disponible y brindarme un apoyo efectivo, aclarándome las dudas que se me presentaron y gestionando más allá de su alcance en mis dilemas.

De antemano muchas gracias.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

pág

RESUMEN

El mundo es una red, actualmente vivimos conectados a internet u otro medio, como Red de celular, televisión, radio, entre otros, es por tal motivo que las telecomunicaciones han implantado un desarrollo notable para la civilización y es de vital importancia tener conocimientos sólidos referente a este tema, el programa Diplomado De Profundización DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN, ofrecido bajo el convenio CISCO Network Acamedy y la Universidad Nacional Abierta y A Distancia (UNAD), me ha permitido mejorar mis habilidades en telecomunicaciones y establecer bases sólidas como futuro Ingeniero De Sistemas; Las temáticas abordadas en el diplomado se dividieron en dos módulos, el primer con el nombre CCNA1 “Introduction to Networks”; en el cual se abordan temas como fundamentos de Networking, Modelo OSI e implementar redes básicas bajo parámetros IP, el segundo CCNA2 “Routing and Switching Essentials”; En el que se abordaron temáticas, configuración de routing y sistemas de red soportados en vlans, configuraciones avanzadas de enrutamiento, tales como RIPV1, RIPV2, OSPF, IGRP, EIGRP, para evaluar la apropiación de dichos conceptos se plantea la Prueba de Habilidades Practica, la cual se desarrolla y explicara paso a paso, a continuación, permitiendo demostrar las habilidades y competencias adquiridas.

PALABRAS CLAVE

Diplomado, Telecomunicaciones, Redes, Router, Switch, protocolos, Prueba.

ABSTRACT

The world is a network, we currently live connected to the internet or other médium, as Cellular network, television, radio, among others, the telecommunications have implemented a remarkable development for civilization and it is vitally important to have solid knowledge regarding this topic, the program DESIGN AND IMPLEMENTATION OF LAN / WAN INTEGRATED SOLUTIONS offered under the agreement CISCO Network Acamedy and Universidad Nacional Abierta y A Distancia (UNAD), has allowed me to improve my communications skills and establish solid foundations as a future Systems Engineer. The topics covered in the course were divided into two modules, the first with the name CCNA1 “Introduction to Networks”; in which fundamental concepts of Networking, Model OSI and implement basic networks under parameters IP, and second CCNA2 “Routing and Switching Essentials”; concepts of configuration of routing and network systems supported in vlans, advanced routing settings, as RIPV1, RIPV2, OSPF, IGRP, EIGRP, to evaluate the concepts it develops the Practice Skills Test the which will be explained step by step then.

1. INTRODUCCION

Las redes y telecomunicaciones siguen actualizándose y por tal motivo la capacitación a nuevos, profesiones es de vital importancia, para mantener y mejorar la conectividad, es por tal motivo que la Universidad Nacional Abierta Y A Distancia UNAD, permite a sus estudiantes tener la posibilidad de adquirir y ratificar conocimientos en dicho campo.

La evaluación “Prueba de Habilidad Practicas”, permite al estudiante ratificar las competencias impartidas en el diplomado PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), de tal manera que se tenga la convicción de crear y administrar redes de datos.

2. OBJETIVOS

2.1 Objetivo General.

Desarrollar de forma exitosa y explicando paso a paso la Prueba de Habilidades Practicas, propuesta en el DIPLOMADO PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).

2.2 Objetivos Específicos.

- Utilizar el software Cisco Packet Tracer, para el desarrollo de los ejercicios propuestos.
- Identificar y utilizar los dispositivos requeridos según cada ejercicio.
- Establecer una red y subred en cada ejercicio, asignando de forma correcta una dirección IP, mascara de red y wildcard, según se requiera.
- Configurar de forma correcta los dispositivos Routers, Switchs, Computadoras, Servidores, según los solicitado en cada escenario, de la Prueba de Habilidades Practicas.
- Establecer conexiones según lo solicitado en cada escenario.
- Verificar el funcionamiento de cada dispositivo según lo solicitado en cada escenario.
- Documentar paso a paso el proceso desarrollado en cada escenario de la Prueba de Habilidades Practicas.

3. PLANTEAMIENTO DEL PROBLEMA

La siguiente prueba de habilidades, permitirá afianzar y ratificar las destrezas que se adquirieron durante todo el transcurso de Diplomado CCNA, PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).

3.1 DEFINICION DEL PROBLEMA

La prueba de habilidades prácticas, hace parte de las actividades, del Diplomado DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), en la cual consiste en el desarrollo de dos escenarios que permitirán demostrar las habilidades que se obtuvieron, para esta actividad el estudiante contara con dos semanas para el desarrollo de la actividad, la cual es de carácter individual y obligatoria.

Para la prueba se podrá desarrollar utilizando alguna de las herramientas Cisco Packet Tracert u GNS3, los cuales son los softwares que se utilizaron durante el transcurso del curso, de tal manera que se debe desarrollar cada escenario haciendo uso de una de estas.

La prueba de habilidades consiste en:

“Dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una

de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros" (UNAD, 2019).

Escenario 1

"Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red". (UNAD, 2019)

Escenario 2

"Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original". (UNAD, 2019)

3.2 JUSTIFICACION

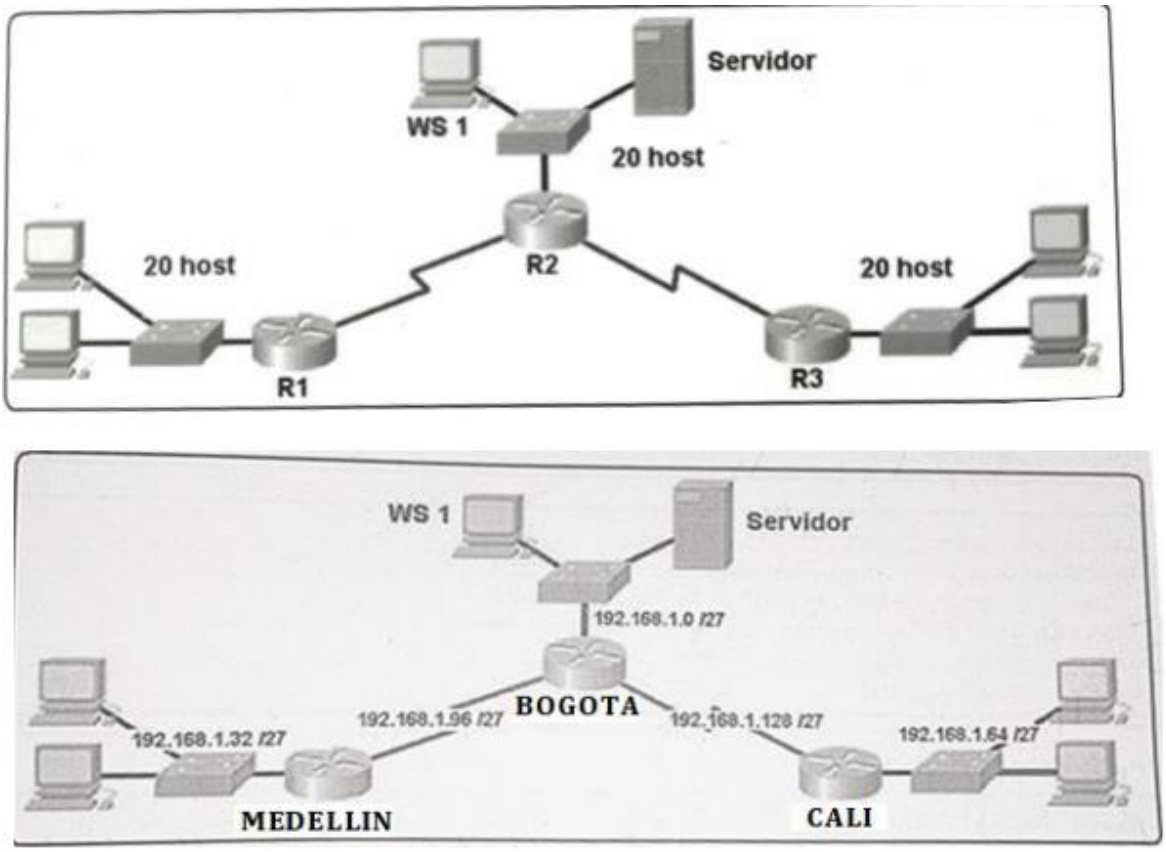
La Universidad Nacional Abierta Y A Distancia, ofrece múltiples opciones de grado, brindando la posibilidad al estudiante de escoger entre las misma, una de las cuales es DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), la cual es una interesante opción ya que permite, mejorar las habilidades y competencias en el campo de redes y telecomunicaciones, sin dejar de lado que es ofrecido por una de las compañías más fuertes en dicho campo CISCO, lo cual garantiza que el contenido del

diplomado este a la vanguardia y genere un atractivo para el estudiante, es debido que esta alternativa de grado es la posibilidad de adquirir conocimientos de alto nivel, para ratificar dichos conceptos se desarrollará paso a paso la Prueba de Habilidades Practicas.

4. DESARROLLO DEL PROYECTO.

4.1. ESCENARIO 1

Figura 1.Escenario Uno



Fuente 1.Escenario uno, Autor: UNAD

Se desarrollará el siguiente escenario dispuesto, para tal efecto se explicará paso a paso el desarrollo del mismo, explicando el procedimiento de forma concisa sin omitir ningún paso llevado a cabo, se evidenciará por medio de imágenes y tablas, acompañadas de una explicación.

La siguiente imagen establece la topología de red, dispuesta para el escenario uno, para el cual se utilizarán host de tipo, router, Servidor y Computadoras de escritorio.

4.1.1. Parte 1 Asignación de direcciones IP:

4.1.1.1 Se debe dividir (subnetear)la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.

Tabla 1. Subnetear Red Clase C

RED CLASE C 192.168.1.0/24 -> 255.255.255.0					
SUBREDES					
N°	SubRed	Primera IP Utilizable	Ultima IP Utilizable	BroadCast	Mascara de Red
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31	255.255.255.224
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63	255.255.255.224
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95	255.255.255.224
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127	255.255.255.224
5	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159	255.255.255.224

6	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191	255.255.255.224
7	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223	255.255.255.224
8	192.168.1.224	192.168.1.225	192.168.1.226	192.168.1.227	255.255.255.224

Fuente 2.prueba de habilidades prácticas, Autor: Javier Bulla

El procedimiento de subneteo consiste en subdividir un dominio de red, en varias fracciones, permitiendo establecer un orden estructurado en una topología sin embargo se pueden desperdiciar muchas direcciones IP, lo cual es una desventaja, al implementar el método de asignación de direcciones IP (Protocolo de Internet).

Se establece un subneteo de la red con dirección IP 192.168.1.0 /24 con mascara de red 255.255.255.0, en ocho partes, para tal efecto se realiza el siguiente procedimiento:

En el cual se subdividió la red en ocho partes, de igual manera, las subredes tienen dominios diferentes pero la misma mascara de red, lo cual permite concluir que son producto de un subneteo, lo cual garantiza que en el transcurso del tiempo se puede amplificar la red.

4.1.1.2 Asignar una dirección IP a la red.

Dirección de red Privada de clase C dirección ip192.168.1.0 mascara de red 255.255.255.0

4.1.2. Parte 2: Configuración Básica:

Tabla 2. Configuración Básica tabla de enrutamiento.

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**

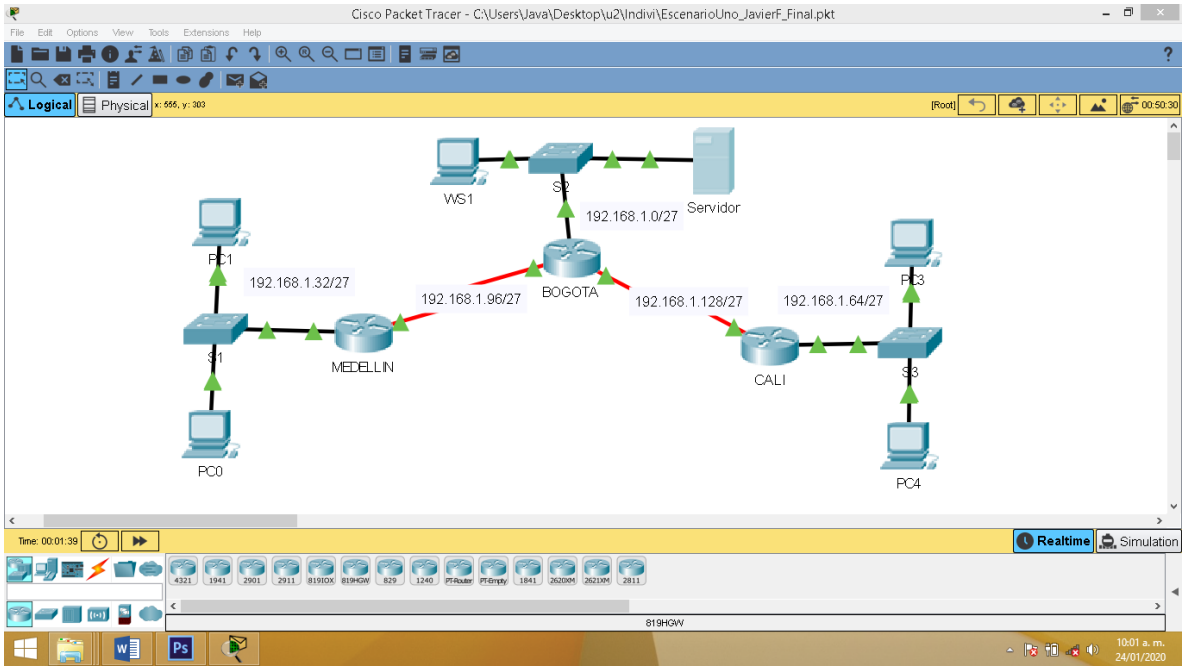
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	---	192.168.1.130	-----
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Fuente 3. prueba de habilidades prácticas, Autor: Javier Bulla

La siguiente tabla permite tener un orden y claridad en las direcciones IP y máscaras de red que se utilizaran en cada dispositivo host de cada subred, de igual manera se establece el protocolo de enrutamiento en el dispositivo de capa tres y el sistema de actualización de la tabla de enrutamiento.

4.1.2.1 Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Figura 2.Esquema de escenario Uno



Fuente 4. prueba de habilidades prácticas, Autor: Javier Bulla

Se construye la red, con los dispositivos que han sido establecidos para el escenario uno, la siguiente implementación, se lleva a cabo por medio del software Cisco Packet Tracert, herramienta suministrada, por la compañía Cisco, la cual se utilizará solo con fines académicos.

Tabla 3. Tabla de Enrutamiento a host de la red

TABLA DE ENRUTAMIENTO				
SUBREDE MEDELLIN				
Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway

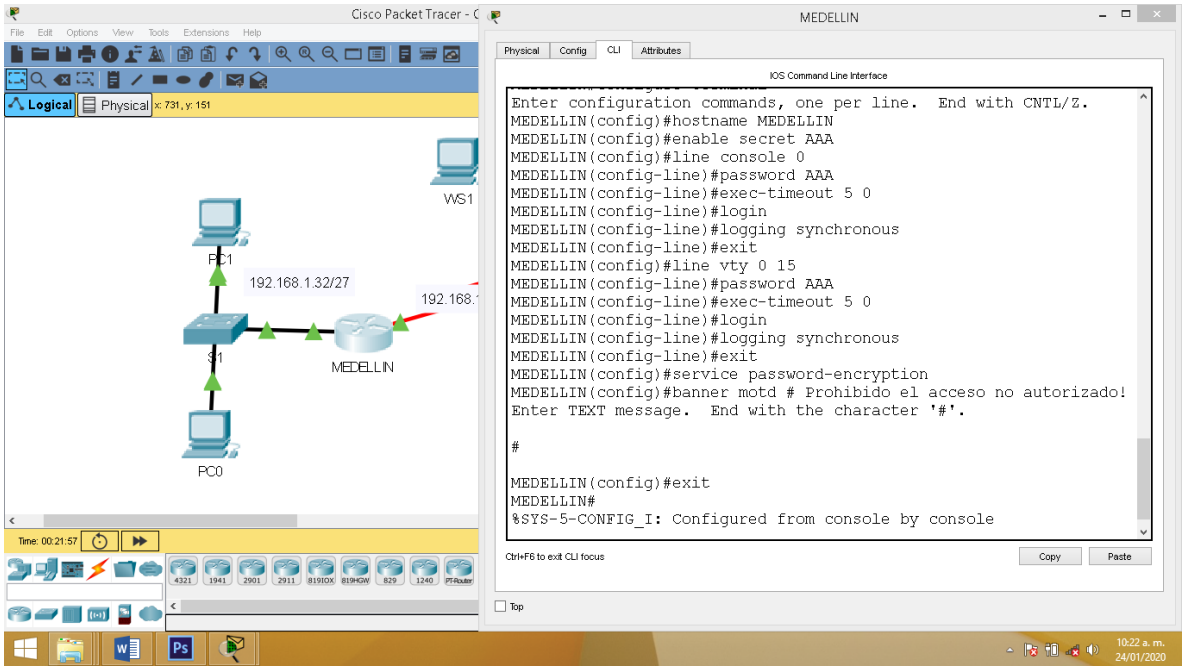
Router (Medellín)	Serial 0/0/0 Clock	192.168.1.99	255.255.255.224	N/C
	G0/0	192.168.1.33	255.255.255.224	N/C
PC0	F0/0	192.168.1.34	255.255.255.224	192.168.1.33
PC1	F0/0	192.168.1.35	255.255.255.224	192.168.1.33
SUBREDE BOGOTA				
Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway
Router (Bogotá)	Serial 0/0/0 Clock	192.168.1.98	255.255.255.224	N/C
	Serial 0/0/1	192.168.1.130	255.255.255.224	N/C
	G0/0	192.168.1.1	255.255.255.224	N/C
Servidor	F0/0	192.168.1.2	255.255.255.224	192.168.1.1
WS1	F0/0	192.168.1.3	255.255.255.224	192.168.1.1
SUBREDE CALI				
Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway
Router (Cali)	Serial 0/0/1	192.168.1.131	255.255.255.224	N/C
	G0/0	192.168.1.65	255.255.255.224	N/C
PC3	F0/0	192.168.1.66	255.255.255.224	192.168.1.65
PC4	F0/0	192.168.1.67	255.255.255.224	192.168.1.65

Fuente 5. prueba de habilidades prácticas, Autor: Javier Bulla

La tabla de enrutamiento permite establecer las direcciones IP, que se establecerán a los dispositivos de la red, esto permite establecer un orden sistemático para no incurrir en errores posteriormente.

Configuración básica de Router Medellín.

Figura 3.Configuración Básica Router Medellín



Fuente 6. prueba de habilidades prácticas, Autor: Javier Bulla

Se llevará a cabo la implementación de una configuración básica en el router Medellín para llevar a cabo esta configuración se ejecutarán los siguientes comandos que se explicarán a continuación.

Comandos:

MEDELLIN> enable

Permite ingresar a el modo de configuración global

MEDELLIN#configure terminal

Permite ingresar a el modo de configuracion

MEDELLIN(config)#hostname MEDELLIN

Permite asignar el nombre a el hots.

MEDELLIN(config)#enable secret AAA

Permite asignar una contraseña a el dispositivo.

Permite establecer solo una linea de consola de acceso.

MEDELLIN(config)#line console 0

MEDELLIN(config)#password AAA

MEDELLIN(config-line)#exec-timeout 3 0

MEDELLIN(config- line)#login

MEDELLIN(config- line)#logging synchronous

MEDELLIN(config)#exit

La configuracion ssh y telnet permiten el ingreso de sección a nivel de privilegio 15

MEDELLIN(config)#line vty 0 15

MEDELLIN(config)#password AAA

Permite establecer un tiempo de acceso.

MEDELLIN(config)#exec-timeout 3 0

MEDELLIN(config)#login

MEDELLIN(config)#logging synchronous

MEDELLIN(config)#exit

Permite que las contraseñas se encripten y no se muestren en forma de texto.

MEDELLIN(config)#service password-encryption

Permite establecer un tiempo e intentos con los que se contara para iniciar sección.

MEDELLIN(config)#login block-for 180 attempts 3 within 120

Permite establecer un mensaje informativo.

MEDELLIN(config)#banner motd # Prohibido el acceso no autorizado! #

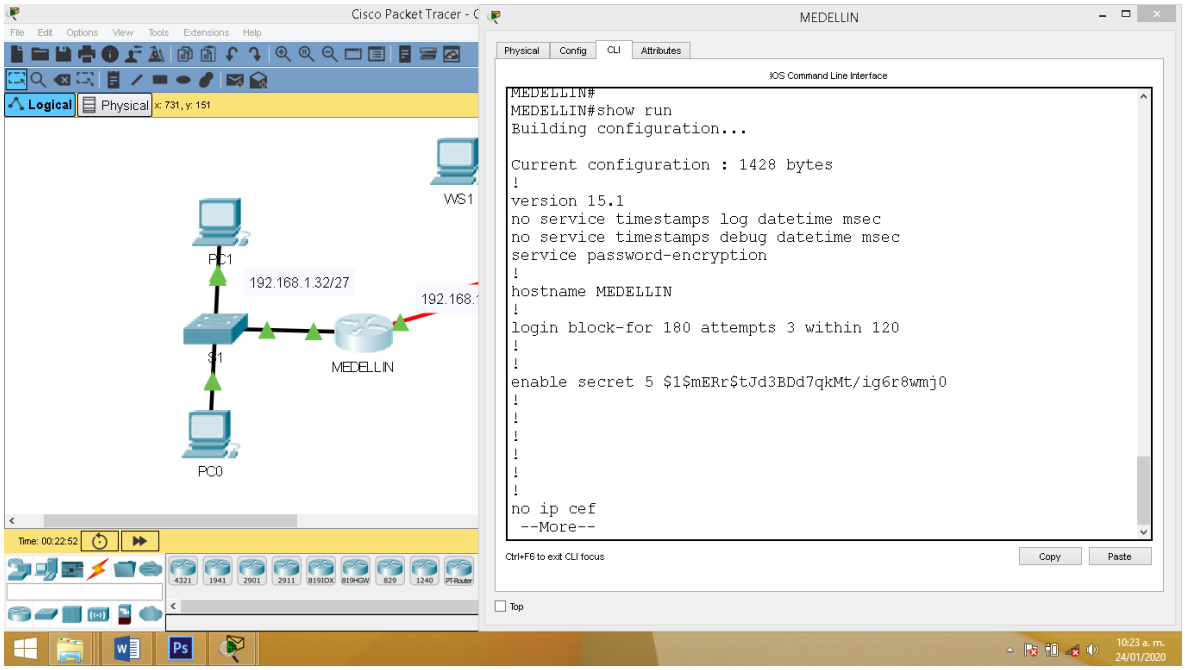
MEDELLIN(config)#exit

Permite guarder la información.

MEDELLIN#copy running-config startup-config

Verificando configuración

Figura 4.Verificación de Configuración de Inicio



Fuente 7. prueba de habilidades prácticas, Autor: Javier Bulla

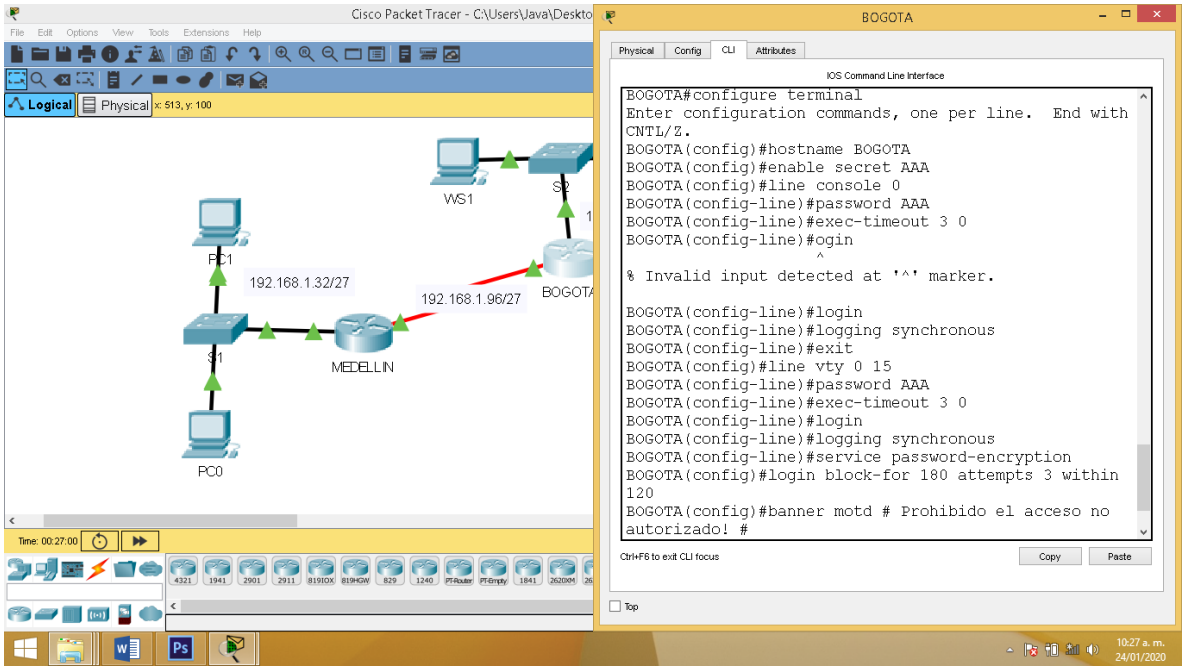
Se verifica la configuración implementada en el dispositivo router Medellín.

Para tal efecto se ejecuta el comando:

MEDELLIN# Show run

Configuración Básica de Router Bogotá

Figura 5.Configuracion Básica de Router Bogotá

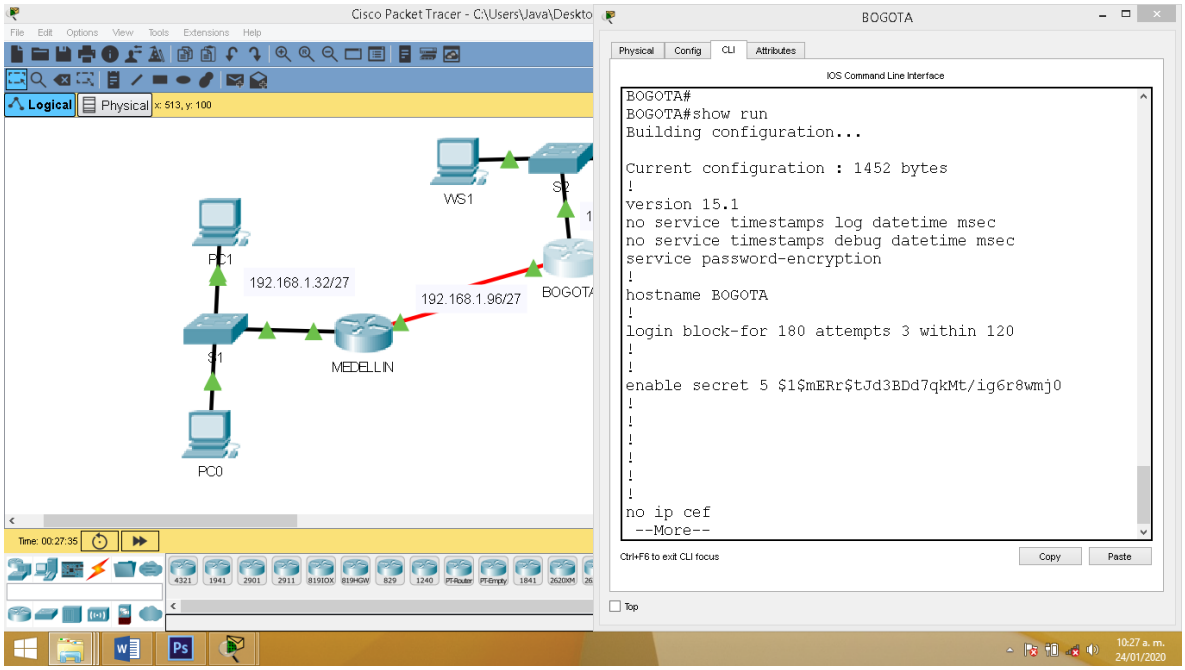


Fuente 8. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo que en el router Medellín, se ejecutan la misma secuencia de comandos en el host Bogotá de tal manera que, se aplica configuración de nombre, contraseñas, encriptación de las misma, tiempo de logueo y banner se realizan la misma para el router Bogotá.

Verificando configuración de Inicio.

Figura 6.Verificando configuración de inicio



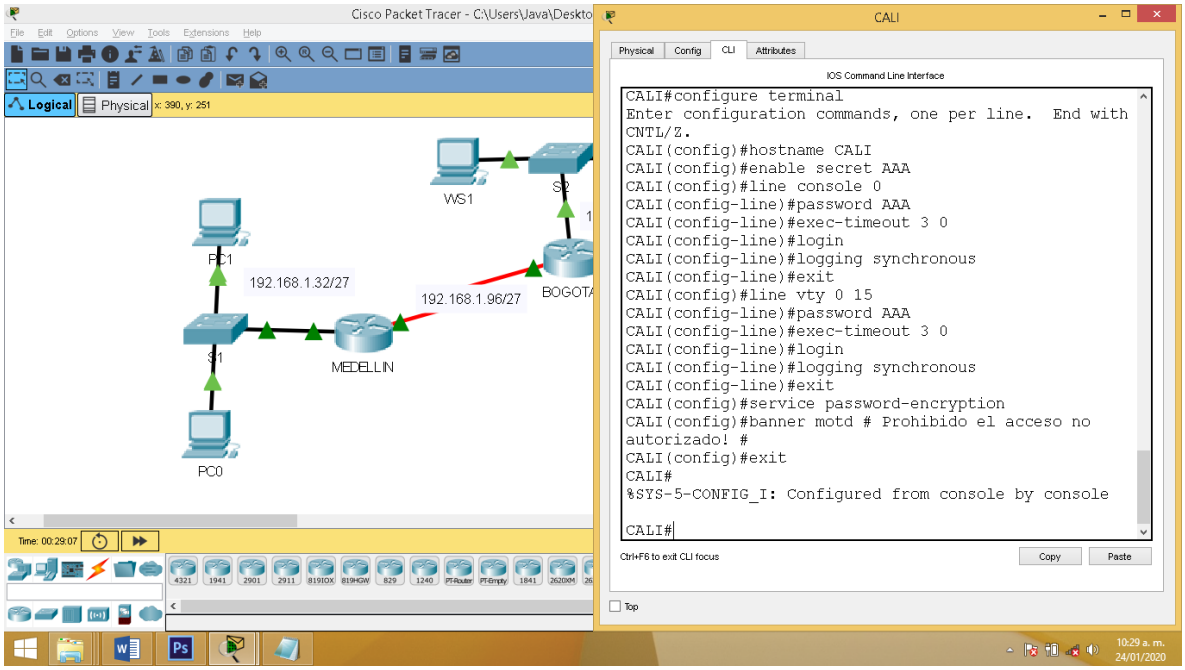
Fuente 9. prueba de habilidades prácticas, Autor: Javier Bulla

Se verifica la configuración realizada en el router Bogotá, para tal efecto se ejecuta el siguiente comando que permite verificar la configuración.

BOGOTA# Show run

Configuración de router Cali.

Figura 7. Configuración básica de Router Cali

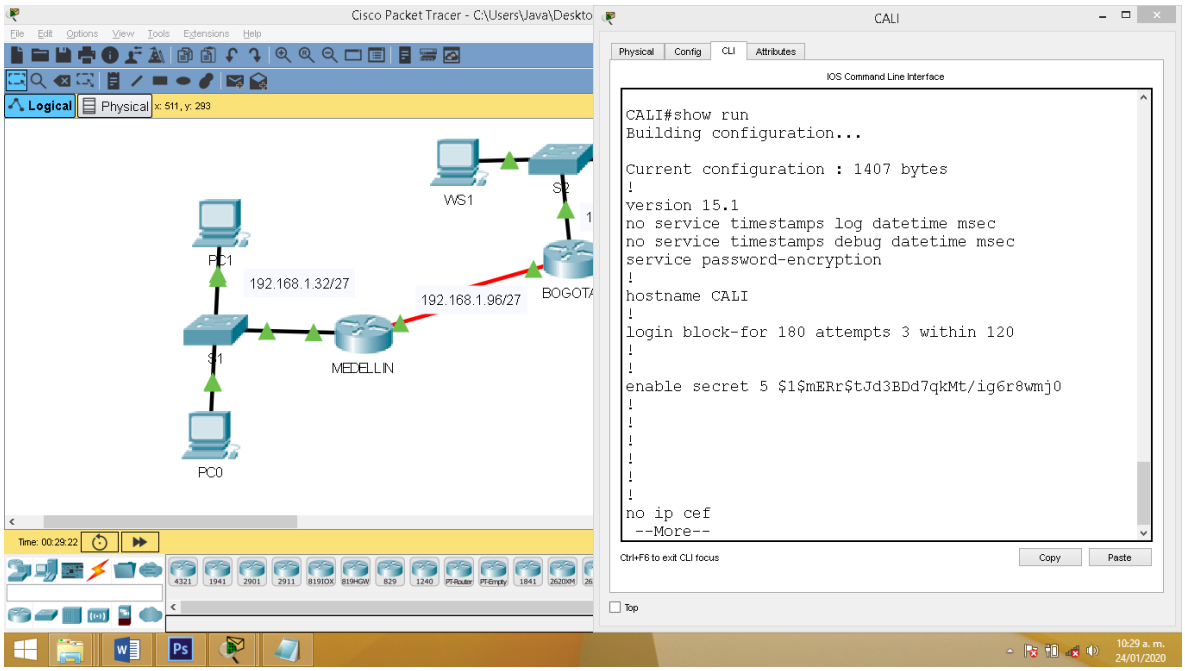


Fuente 10. prueba de habilidades prácticas, Autor: Javier Bulla

Para finalizar se realiza la configuración a el router Cali con los siguientes parámetros; Nombre, contraseñas, encriptación de las misma, tiempo de logueo y banner.

Verificando configuración de Inicio.

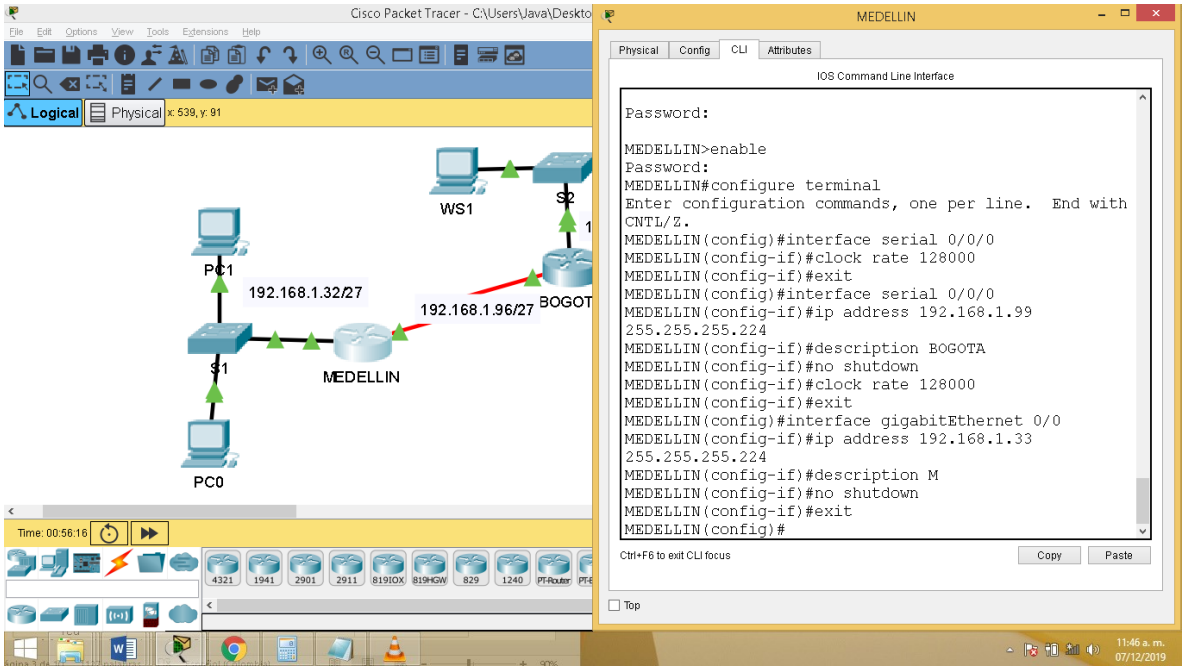
Figura 8.Verificación de configuración de inicio



Fuente 11. prueba de habilidades prácticas, Autor: Javier Bulla

Configuración IP de router Medellín.

Figura 9. Configuración dirección IP router Medellín



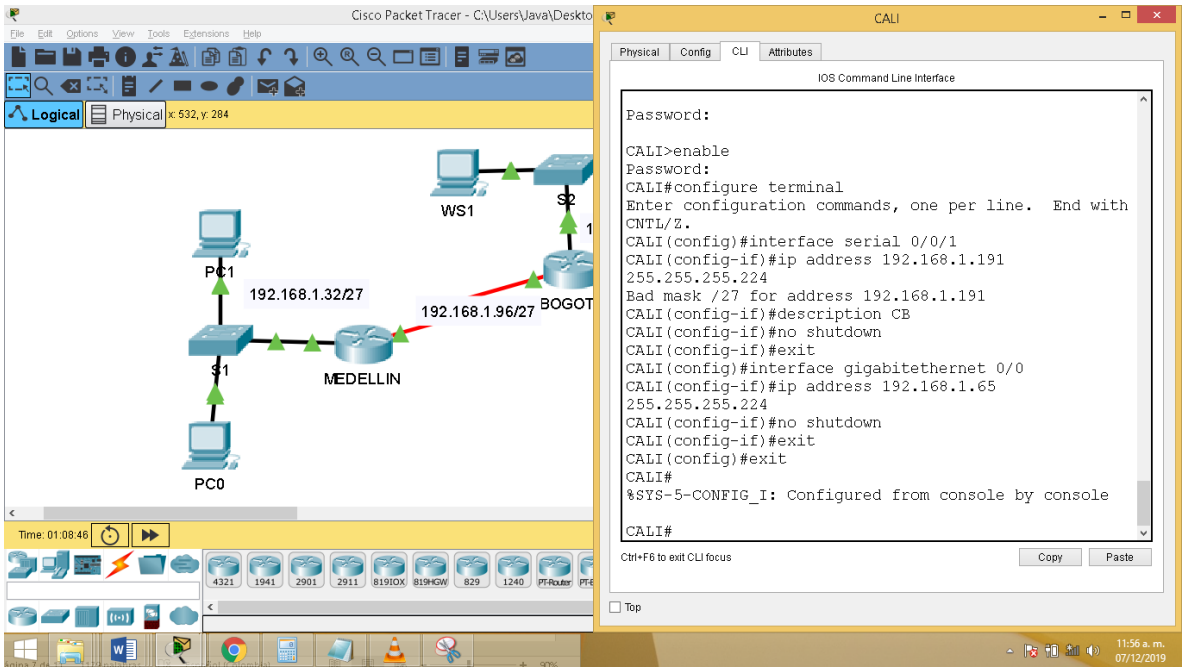
Fuente 12. prueba de habilidades prácticas, Autor: Javier Bulla

Se configura la dirección IP para la interfaz serial s0/0/0 con la siguiente IP 192.168.1.99 y mascara de red 255.255.255.224.

Se configura la interfaz Gigabit Eternet 0/0 con la dirección IP 192.168.1.33 y mascara de red 255.255.255.224.

Configuración Dirección IP router Bogotá.

Figura 10. Configuración dirección IP router Bogotá



Fuente 13. prueba de habilidades prácticas, Autor: Javier Bulla

Se realizan las siguientes configuraciones para el dispositivo router Bogotá, para el cual:

La interfaz serial 0/0/1 tiene la dirección IP 192.168.1.130 con mascara de red 255.255.255.224.

La interfaz Serial 0/0/0 tiene la dirección IP 192.168.1.98 con mascara de red 255.255.255.224.

La interfaz GigabitEthernet 0/0 tiene la dirección IP 192.168.1.1 con mascara de red 255.255.255.224.

BOGOTA(config)#interface g0/0

BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224

BOGOTA(config-if)#no shutdown

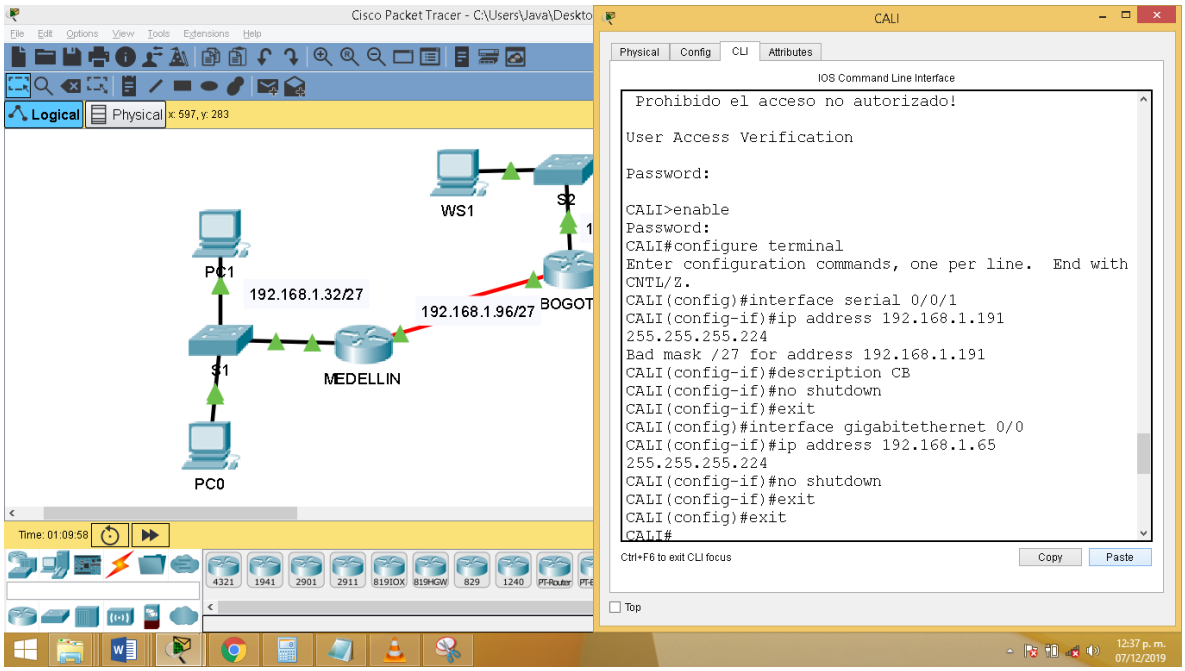
BOGOTA(config)#interface s0/0/1

BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224

BOGOTA(config-if)#clok rate 56000

Configuración dirección IP router Cali

Figura 11. Configuración IP router Cali



Fuente 14. prueba de habilidades prácticas, Autor: Javier Bulla

Se realiza la configuración de dirección IP en las siguientes interfaces del router Cali.

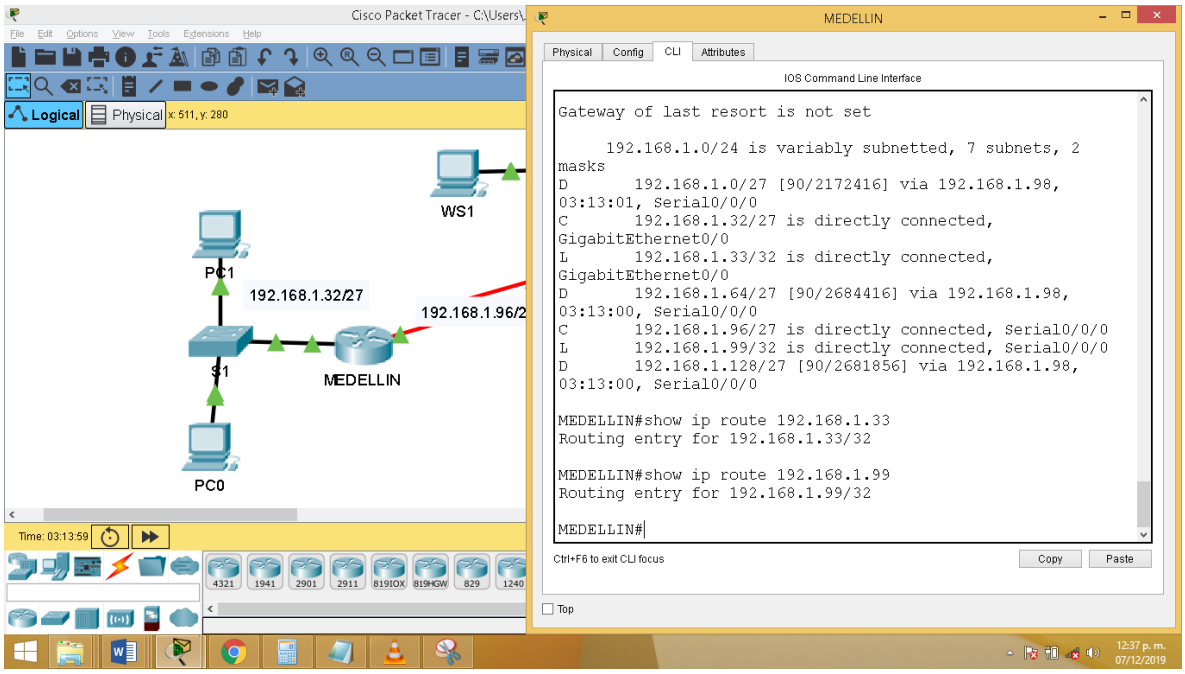
Interfaz serial 0/0/1 con la dirección ip 192.168.1.131 y mascara de red 255.255.255.224

La interfaz gigabitEthernet 192.168.1.65 y mascara de red 255.255.255.224.

4.1.2.2 Verificar el balanceo de carga que presentan los routers.

Verificando balanceo Router Medellín.

Figura 12. Verificando Balanceo router Medellín



Fuente 15. prueba de habilidades prácticas, Autor: Javier Bulla

El balanceo permite verificar, los dispositivos vecinos, de un dispositivo capa tres, para tal efecto router Medellin.

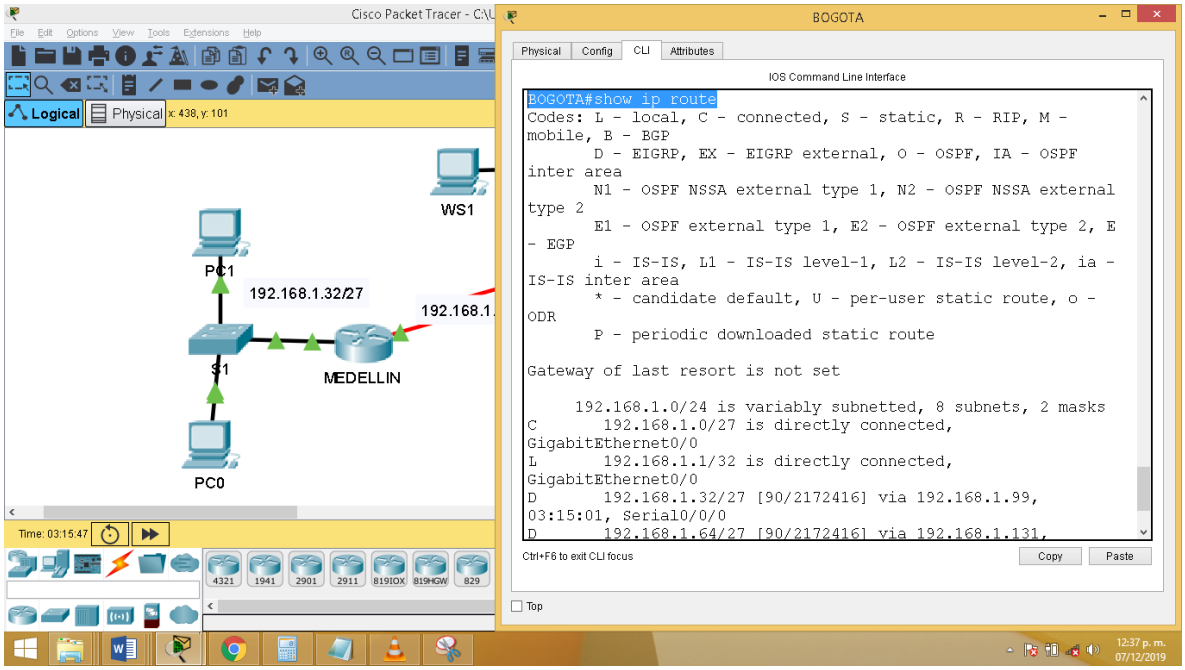
Para verificar el balanceo que dispone el router se ejecuta el comando:

MEDELLIN#show ip route

El cual permite verificar las direcciones locales con las que cuenta el router, según las interfaces que tiene conectadas.

Verificando balanceo Router Bogotá.

Figura 13. Verificando Balanceo router Bogotá



Fuente 16. prueba de habilidades prácticas, Autor: Javier Bulla

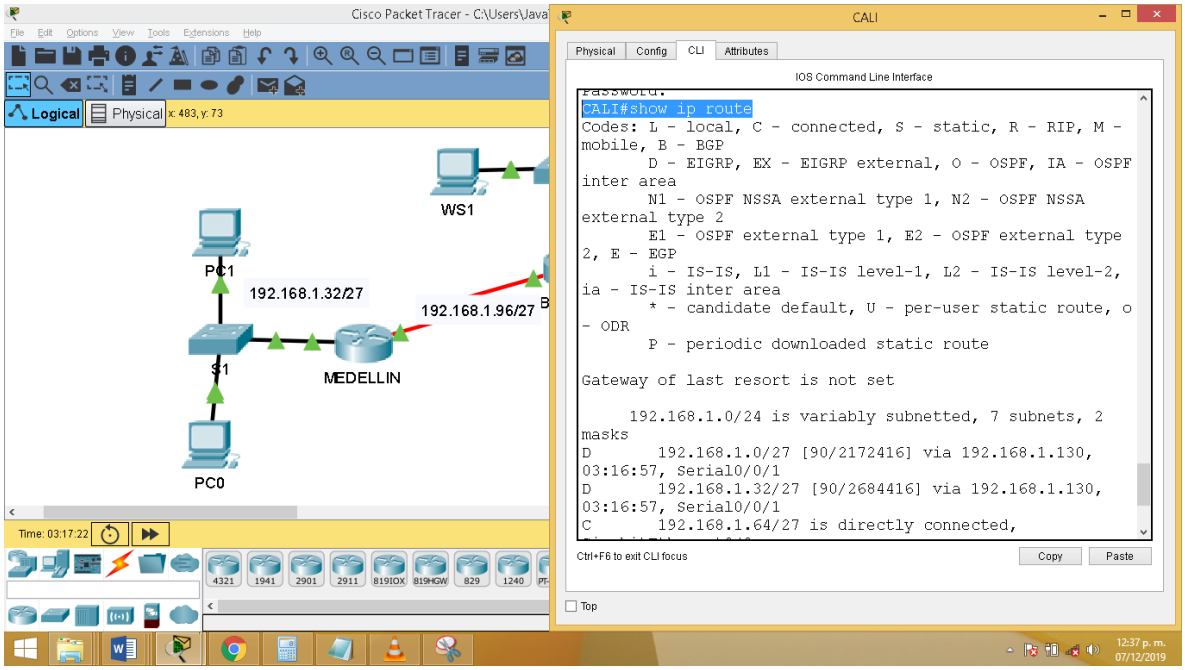
De igual modo que el route Medellín se realiza la verificación de balanceo que dispone el router se ejecuta el comando:

BOGOTA#show ip route

El cual permite verificar las direcciones locales con las que cuenta el router, según las interfaces que tiene conectadas.

Verificando balanceo Router Cali.

Figura 14. Verificando Balanceo router Cali



Fuente 17. prueba de habilidades prácticas, Autor: Javier Bulla

Para finalizar se realiza la verificación de balanceo en el router Cali, para tal efecto se ejecuta el siguiente comando:

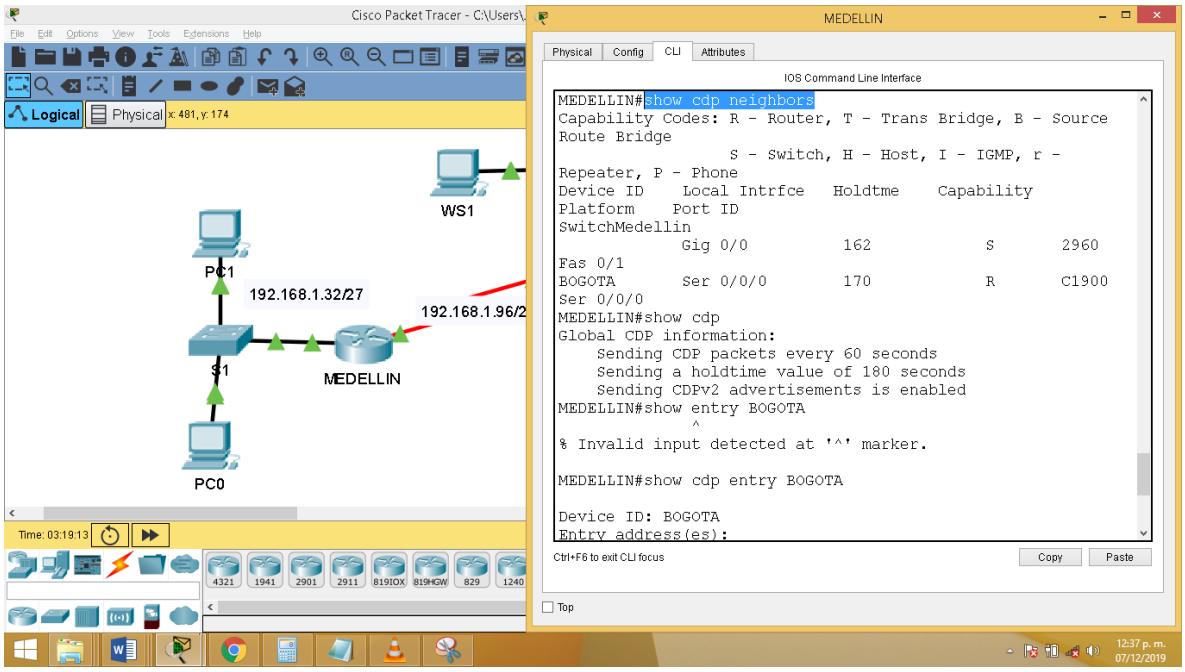
CALI#show ip route

De igual modo se puede visualizar las direcciones IP, que fueron configuradas a las interfaces que dispone el router.

4.1.2.3 Realizar un diagnóstico de vecinos usando el comando cdp.

Verificando Información por Protocolo CDP en router MEDELLIN

Figura 15. CDP router Medellín



Fuente 18. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar los vecinos con los que cuenta un dispositivo router o switch se ejecuta el siguiente comando:

MEDELLIN#show cdp neighbors

Comando que permite verificar los dispositivos con los que esta conectados el dispositivo router.

MEDELLIN#show cdp

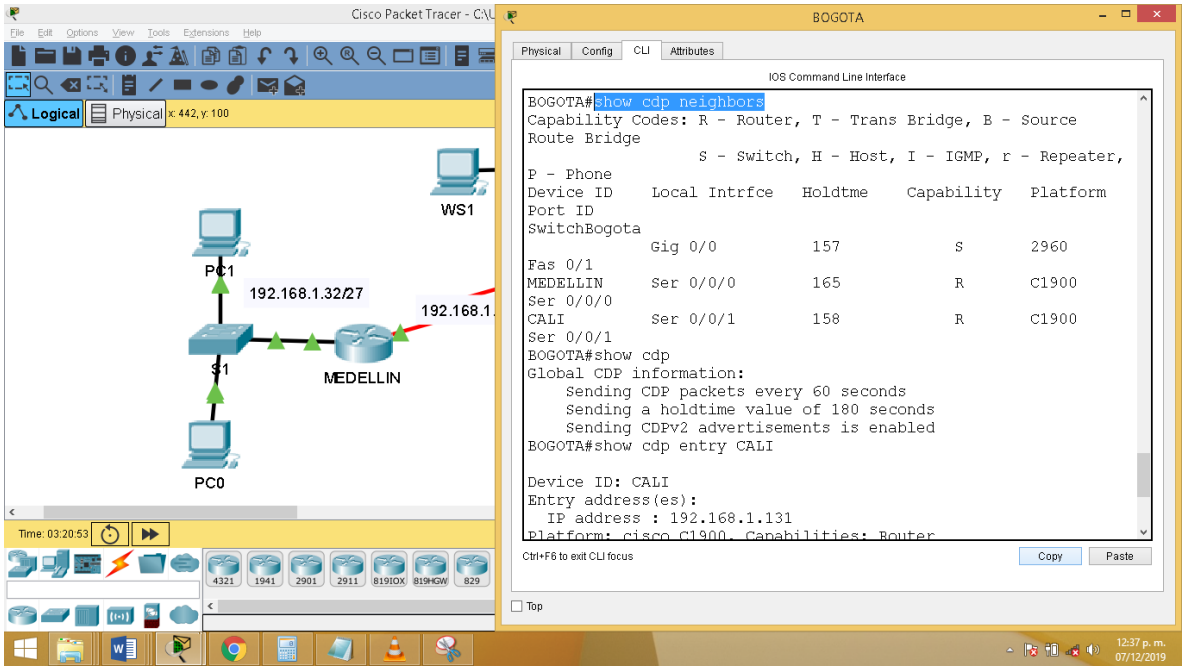
Permite verificar en que lapsos de tiempo se actualiza o descarta un vecino de un dispositivo cisco.

Para verificar la información detallada de cada dispositivo vecino se ejecuta el comando:

MEDELLIN#show cdp entry BOGOTA

Verificando Información por Protocolo CDP en router BOGOTA

Figura 16. CDP router Bogotá



Fuente 19. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar los vecinos del router Bogotá se ejecuta el comando CDP.

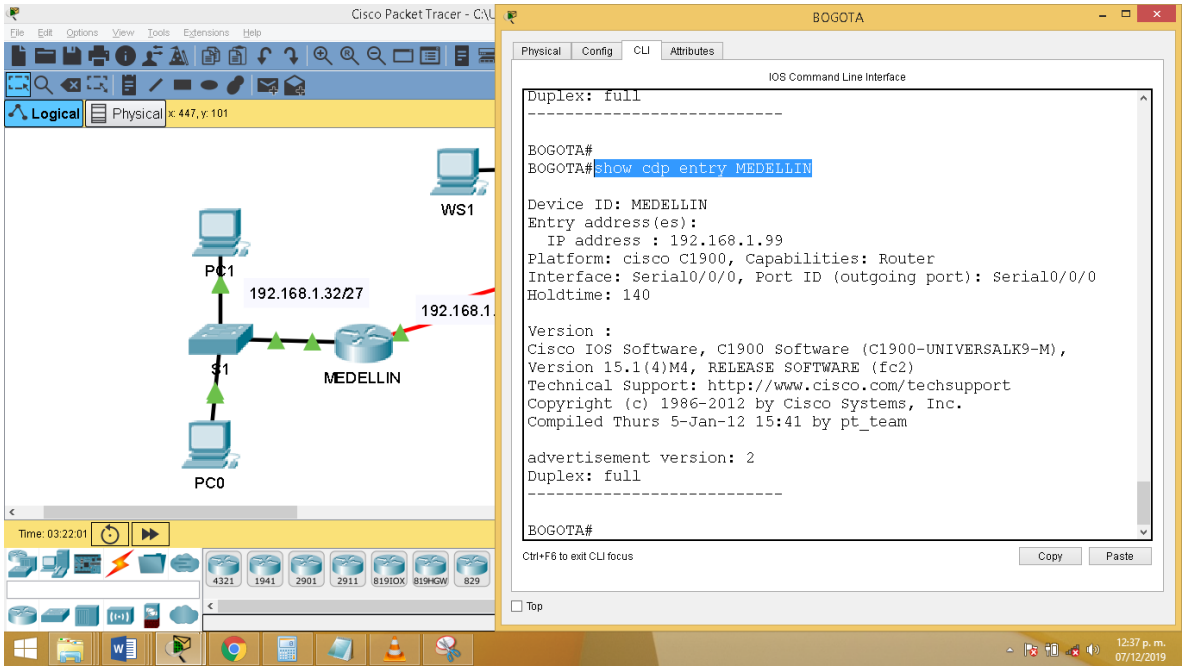
BOGOTA#show cdp neighbors

De igual modo se buscará información detallada de cada vecino para ello se ejecuta el comando:

BOGOTA#show cdp entry BOGOTA

En el cual se mostrar la información detallada del dispositivo router de nombre CALI

Figura 17. CDP router Bogotá



Fuente 20. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo se ejecuta el comando CDP para verificar información detallada de los demás dispositivos vecinos con los que cuenta el router, para ello se ejecutan los siguientes comandos:

BOGOTA#show cdp entry MEDELLIN

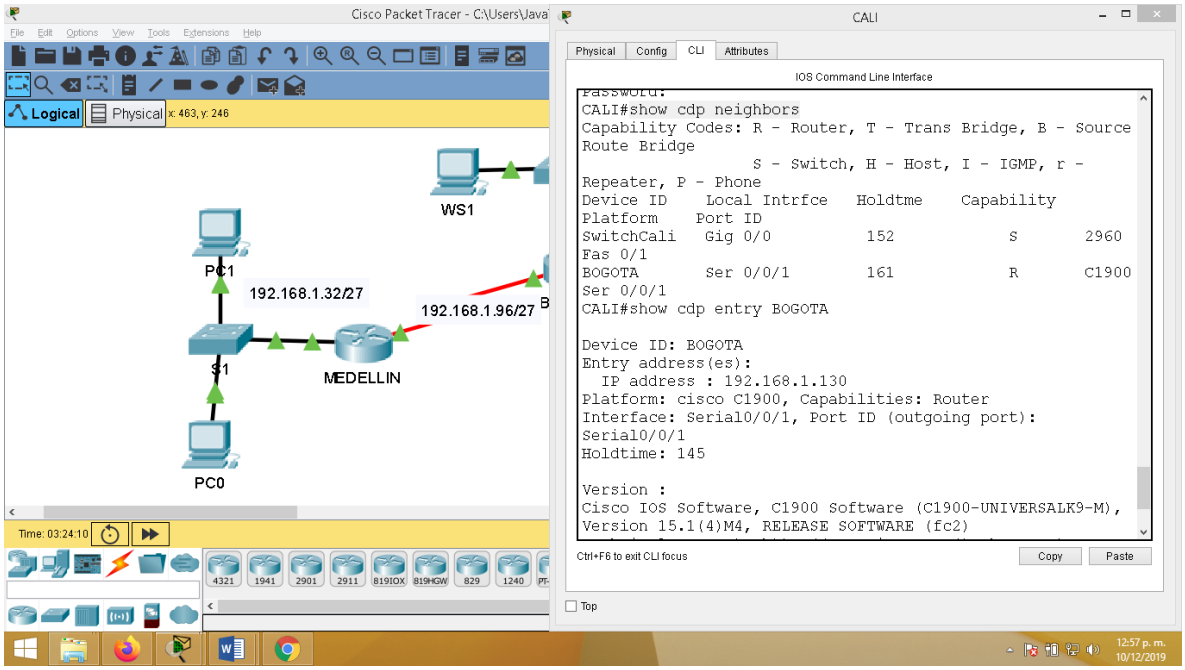
Permite verificar información detalla del host MEDELLIN

BOGOTA#show cdp entry SwitchBogota

Permite verificar información detallada del host SwitchBogota

Verificando Información por Protocolo CDP en router CALI

Figura 18. CDP router Cali.



Fuente 21. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar los vecinos del router Cali, se ejecuta el comando:

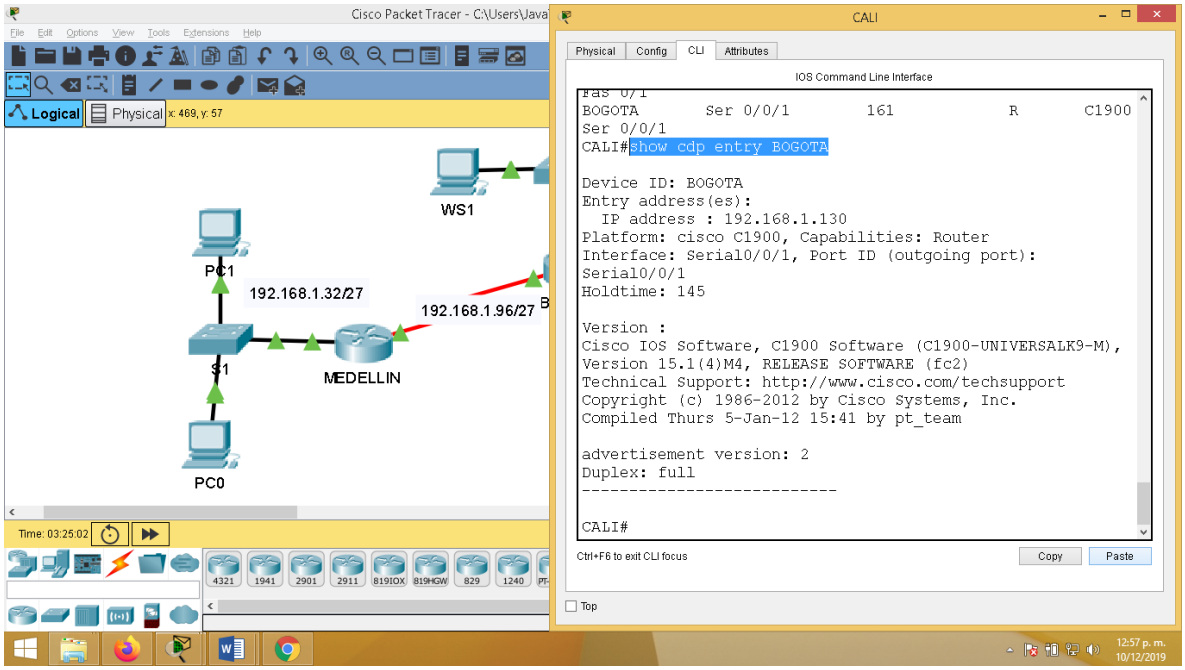
CALI#show cdp neighbors

Permite establecer los vecinos del router Cali.

Para verificar información detallada de cada vecino se ejecuta el siguiente comando:

CALI#show cdp entry BOGOTA

Figura 19. CDP router Cali.



Fuente 22. prueba de habilidades prácticas, Autor: Javier Bulla

CALI#show cdp entry BOGOTA

Permite establecer información detallada del dispositivo BOGOTA

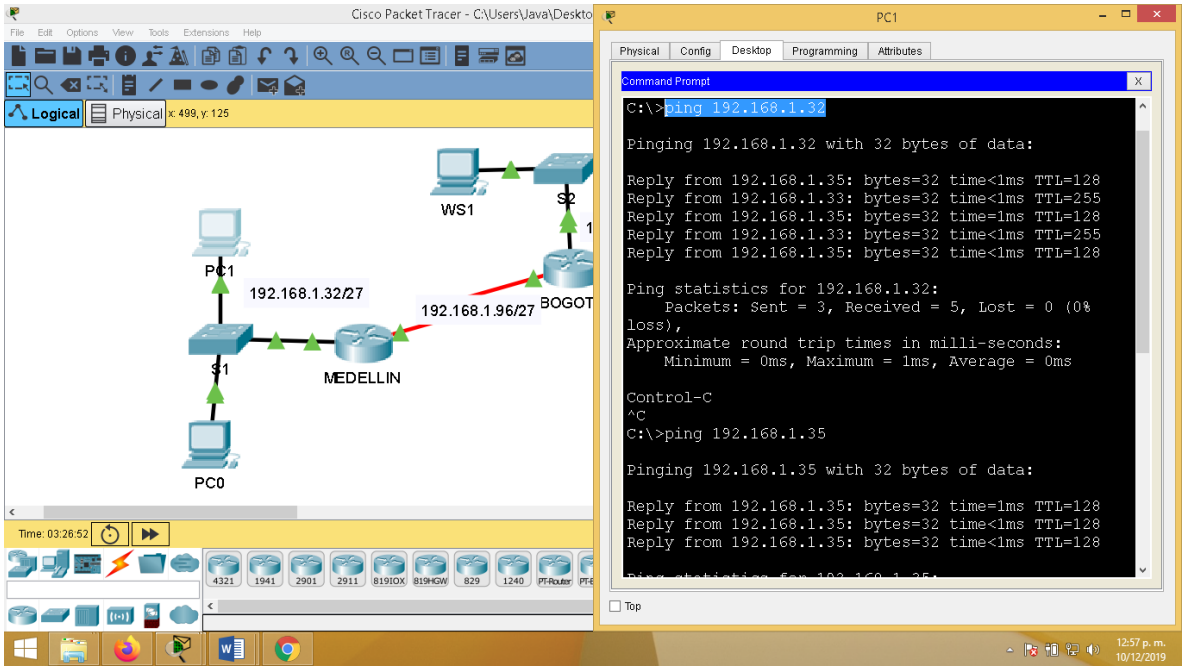
CALI#show cdp entry SwitchCali

Permite establecer información detallada del dispositivo SwitchCali.

4.1.2.4 Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Verificando conectividad en cada trama de la red circulo Azul conjunto M

Figura 20. Verificando conectividad PC1



Fuente 23. prueba de habilidades prácticas, Autor: Javier Bulla

Se puede verificar que la conectividad de la computadora PC1 de la subred de Bogotá, es exitoso.

Para verificar la conectividad en el dispositivo PC1, se ejecuta el comando Ping, para tal efecto:

Tabla 4. Resultados PING entre host

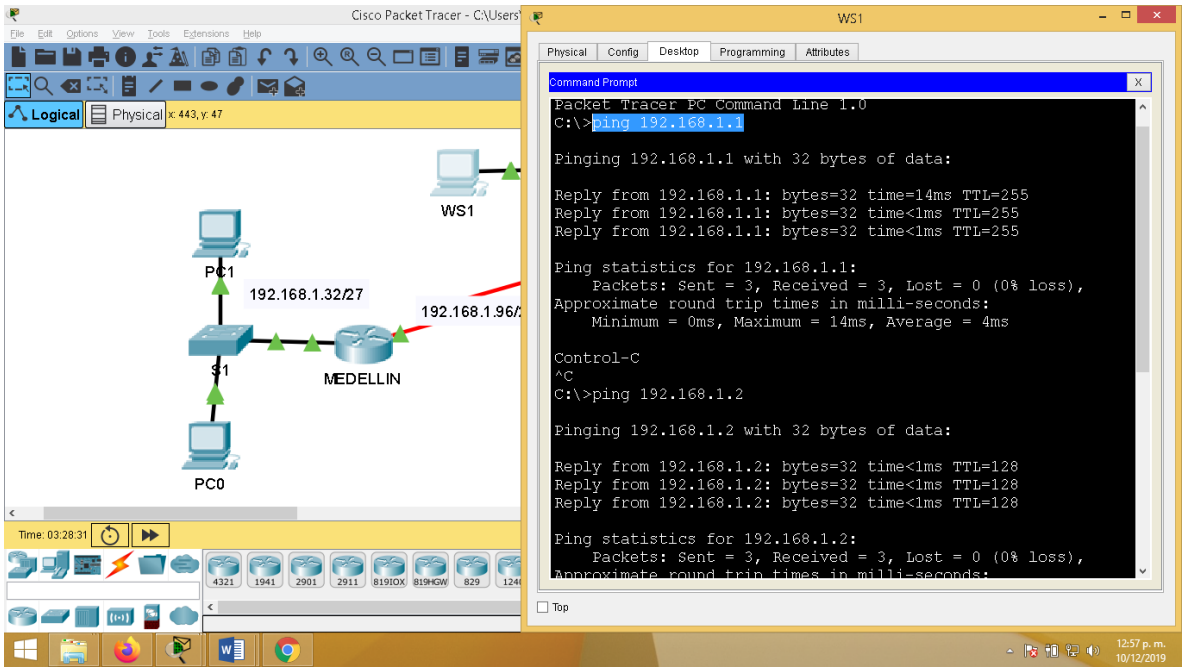
Comando PING PC1	
Comando	Resultado
C:\>ping 192.168.1.33	Exitoso
C:\>ping 192.168.1.35	Exitoso
C:\>ping 192.168.1.99	Exitoso
C:\>ping 192.168.1.98	Fallido

Fuente 24. prueba de habilidades prácticas, Autor: Javier Bulla

Son exitosos los resultados ping en todas las interfaces que se encuentran ubicada en la subred Medellín, para que el router Medellín establezca conexión con los demás hosts externos, "host de las subredes de Bogota y Cali", se debe implementar un protocolo de enrutamiento.

Verificando conectividad en cada trama de la subred Bogotá.

Figura 21. Verificando conectividad WS1



Fuente 25. prueba de habilidades prácticas, Autor: Javier Bulla.

Se puede verificar que la conexión es correcta entre el dispositivo WS1 y los demás host de la red.

Para verificar la conectividad que tiene los dispositivos conectados de la intranet Bogota se ejecuta el comando ping.

Tabla 5. Resultados PING

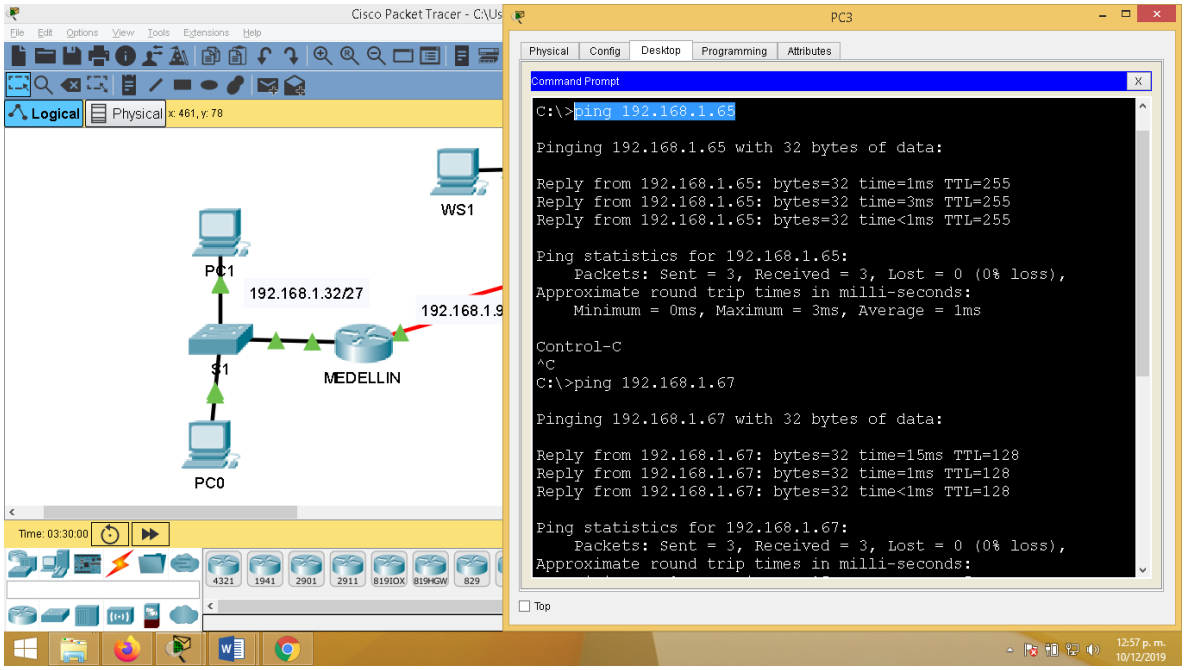
Comando PING PC1	
Comando	Resultado
C:\>ping 192.168.1.1	Exitoso
C:\>ping 192.168.1.2	Exitoso
C:\>ping 192.168.1.98	Exitoso
C:\>ping 192.168.1.99	Fallido

Fuente 26. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo solo hay conectividad en los dispositivos que están contenidos en la subred Bogotá, cuando se realiza un comando ping, a dispositivos o interfaces externas el resultado es fallido.

Verificando conectividad en cada trama de la subred Cali

Figura 22. verificando conectividad PC3



Fuente 27. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la conectividad en los dispositivos que están contenidos en intranet de Cali se ejecuta el comando ping.

Tabla 6. Resultados PING

Comando PING PC1	
Comando	Resultado
C:\>ping 192.168.1.65	Exitoso
C:\>ping 192.168.1.67	Exitoso
C:\>ping 192.168.1.131	Exitoso
C:\>ping 192.168.1.130	Fallido

Fuente 28. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo que en los anteriores casos solo hay conectividad en los dispositivos que están dentro de la figura verde, cuando se realiza el comando ping, externamente el resultado es fallido.

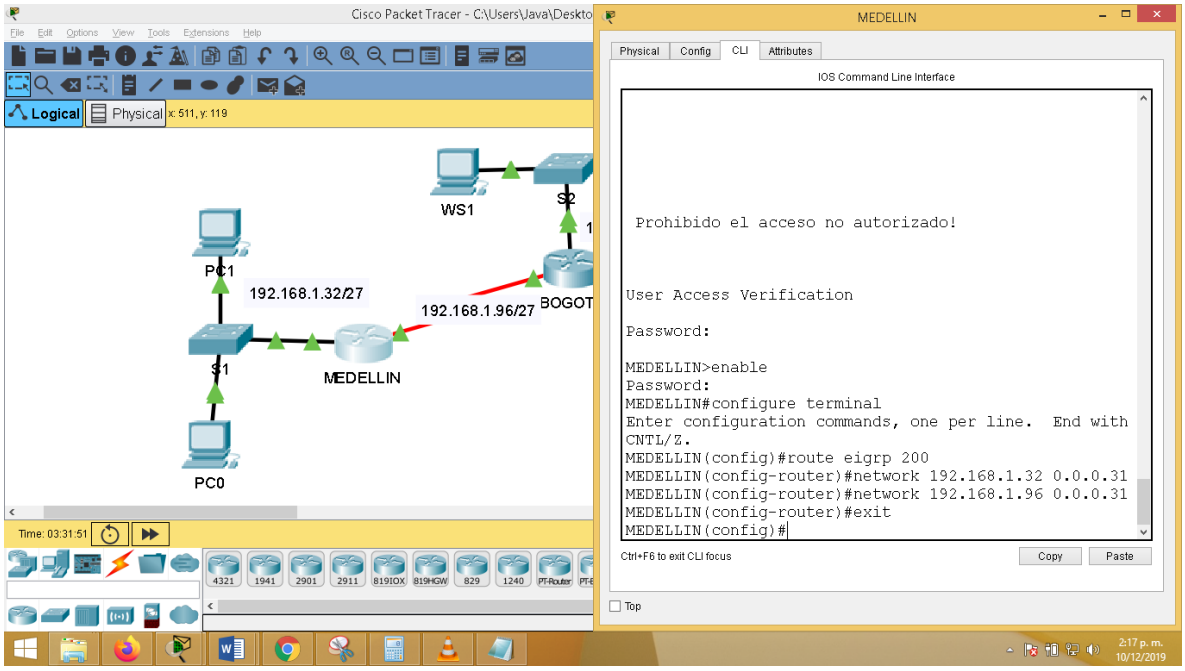
Cabe anotar que no hay conexión entre router, por consiguiente, no es necesario realizar la prueba puesto que ya se conoce de antemano que no hay conexión en los mismo porque un no se ha establecido un protocolo de enrutamiento y los routers no conocen las redes externas.

4.1.3. Parte 3: Configuración de Enrutamiento.

4.1.3.1 Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Protocolo EIGRP en router Medellín

Figura 23. EIGRP router Medellín



Fuente 29. prueba de habilidades prácticas, Autor: Javier Bulla

Se implementa el protocolo EIGRP para que los dispositivos tengan conectividad entre subredes.

Para establecer un protocolo de enrutamiento EIGRP en el router de Medellín, se ejecutan los siguientes comandos:

MEDELLIN>enable

Password:

MEDELLIN#*configure terminal*

MEDELLIN(config)#*router eigrp 200*

MEDELLIN(config-router)#*network 192.168.1.32 0.0.0.31*

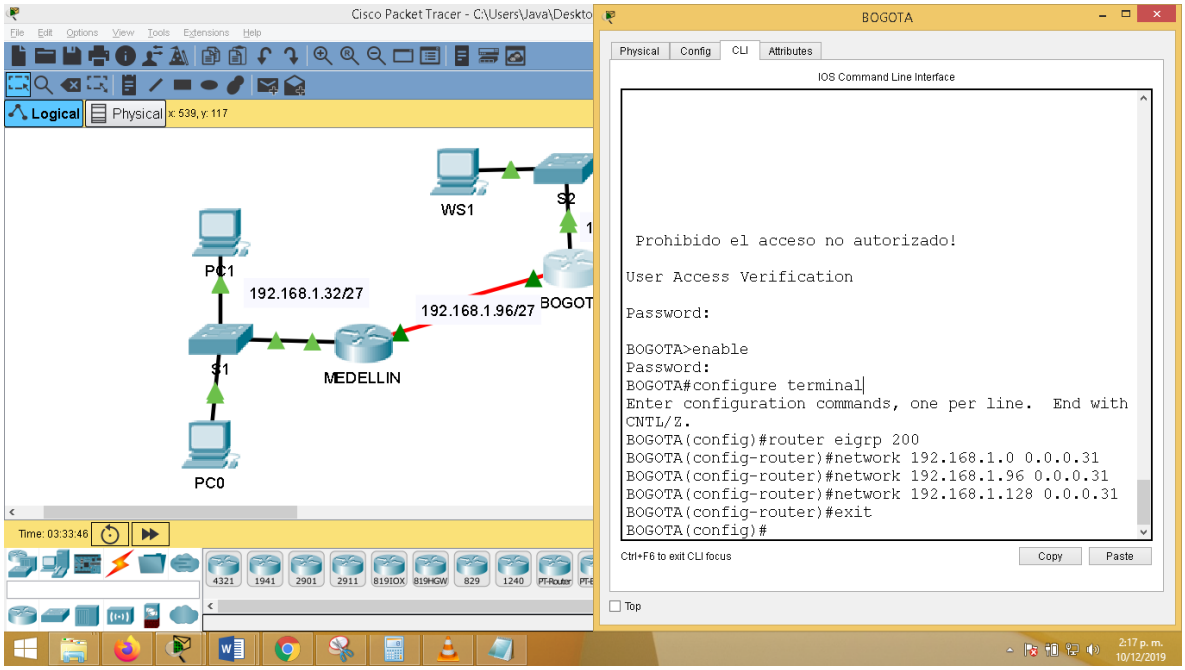
MEDELLIN(config-router)#*network 192.168.1.96 0.0.0.31*

MEDELLIN(config-router)#*exit*

Protocolo EIGRP en router Bogotá.

Para finalizar la implementación del protocolo de enrutamiento EIGRP, se guardan las configuraciones previamente implementadas.

Figura 24. EIGRP router Bogotá



Fuente 30. prueba de habilidades prácticas, Autor: Javier Bulla.

De igual modo que en el router Medellín, se estableció la configuración EIGRP, se procede a implementar el protocolo EIGRP para ser compatible con el implementado en el router Medellín, para llevar a cabo se ejecuta los siguientes comandos en el router Bogotá.

BOGOTA(config)#*router eigrp 200*

BOGOTA(config-router)#*network 192.168.1.0 0.0.0.31*

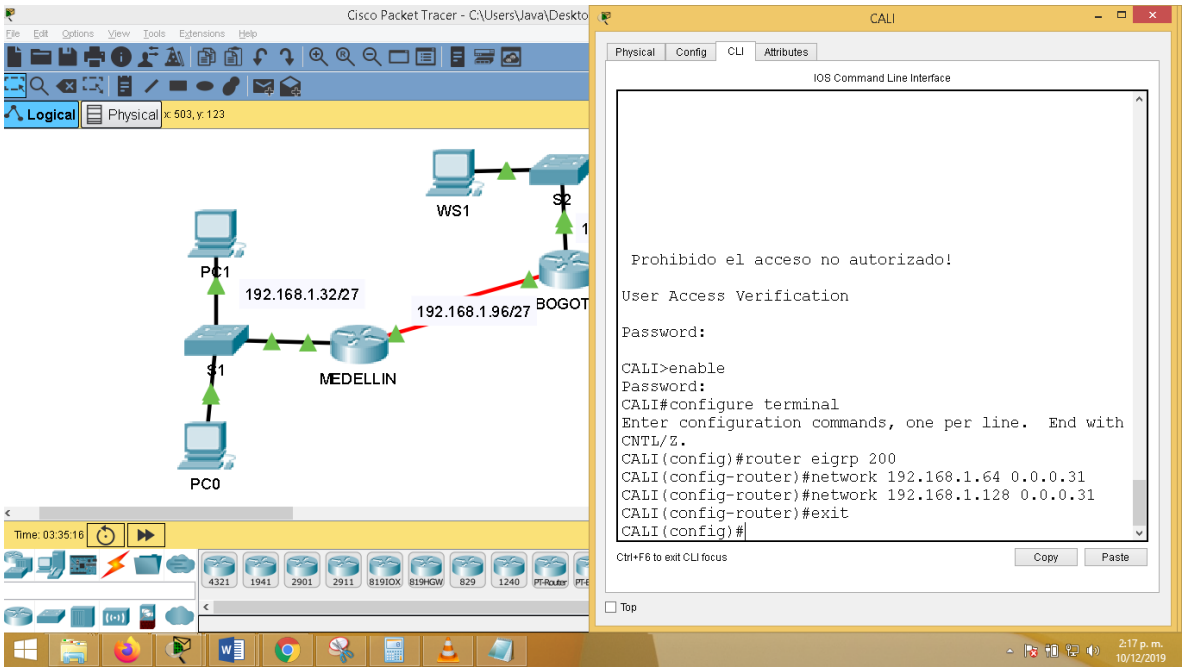
BOGOTA(config-router)#*network 192.168.1.96 0.0.0.31*

BOGOTA(config-router)#*network 192.168.1.128 0.0.0.31*

BOGOTA(config-router)#*exit*

Protocolo EIGRP en router Cali.

Figura 25. EIGRP router Cali



Fuente 31. prueba de habilidades prácticas, Autor: Javier Bulla

Para finalizar el enrutamiento por EIGRP, se procede a configurar el router Cali, para ello se ejecutan los siguientes comandos:

CALI(config)#*router eigrp 200*

CALI(config-router)#*network 192.168.1.64 0.0.0.31*

CALI(config-router)#*network 192.168.1.128 0.0.0.31*

CALI(config-router)#*exit*

De tal manera que las rutas de enrutamiento de ida y vuelta quedan previamente implementadas y funcionando.

4.1.3.2 Verificar si existe vecindad con los routers configurados con EIGRP.

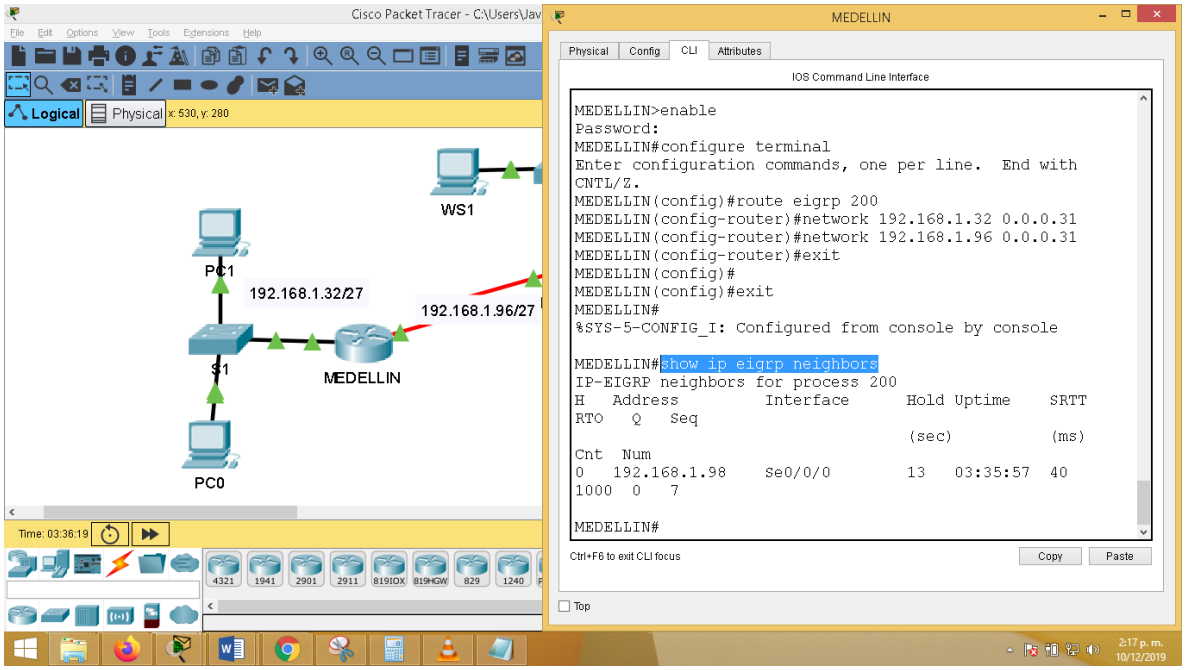
Verificando vecindad EIGRP en router Medellín.

Para tal efecto se ejecuta el comando en modo provilegiado

MEDELLIN#show ip eigrp neighbors

MEDELLIN#show dcp neighbors

Figura 26. Vecindad EIGRP router Medellín.



Fuente 32. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar que la correcta implementación del protocolo EIGRP, se procede a ejecutar el siguiente comando:

MEDELLIN#show ip eigrp neighbors

De igual modo se puede verificar que hay vecindad con un dispositivo de IP 192.168.1.98, el cual es el router Bogotá

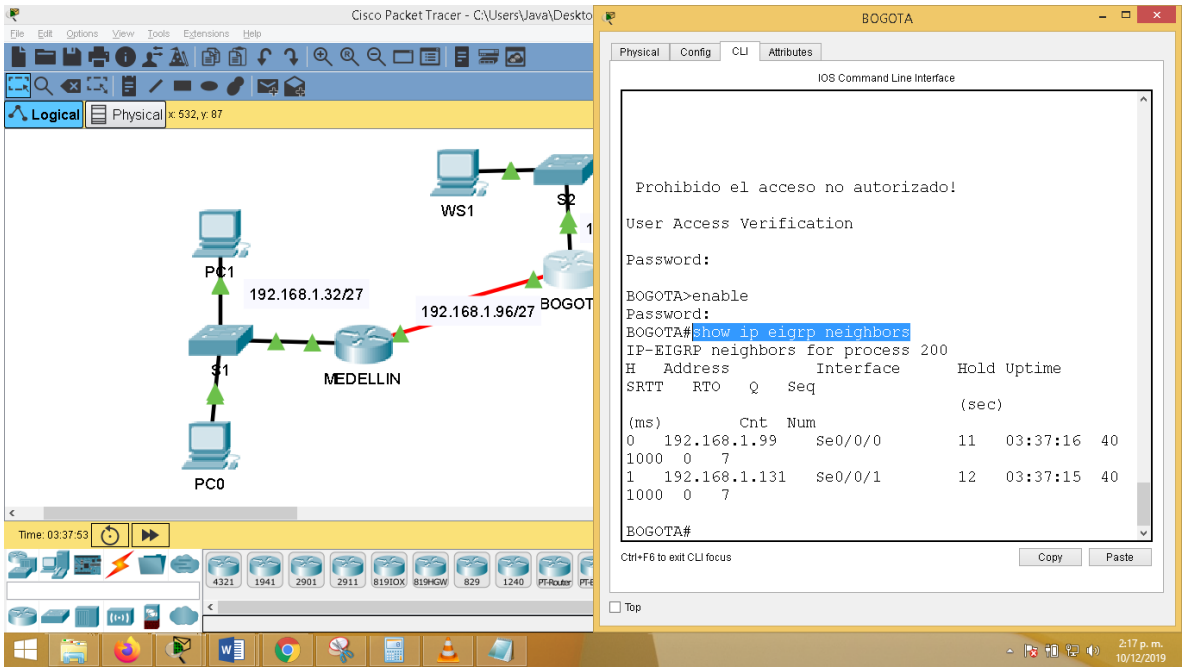
Verificando vecindad EIGRP en router Bogotá

para tal efecto se ejecutan los siguientes comandos.

BOGOTA#show ip eigrp neighbors

BOGOTA #show dcp neighbors

Figura 27. Vecindad EIGRP router Bogotá



Fuente 33. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo para verificar la vencidad del router Bogotá en EIGRP se ejecuta el comando:

BOGOTA#show ip eigrp neighbors

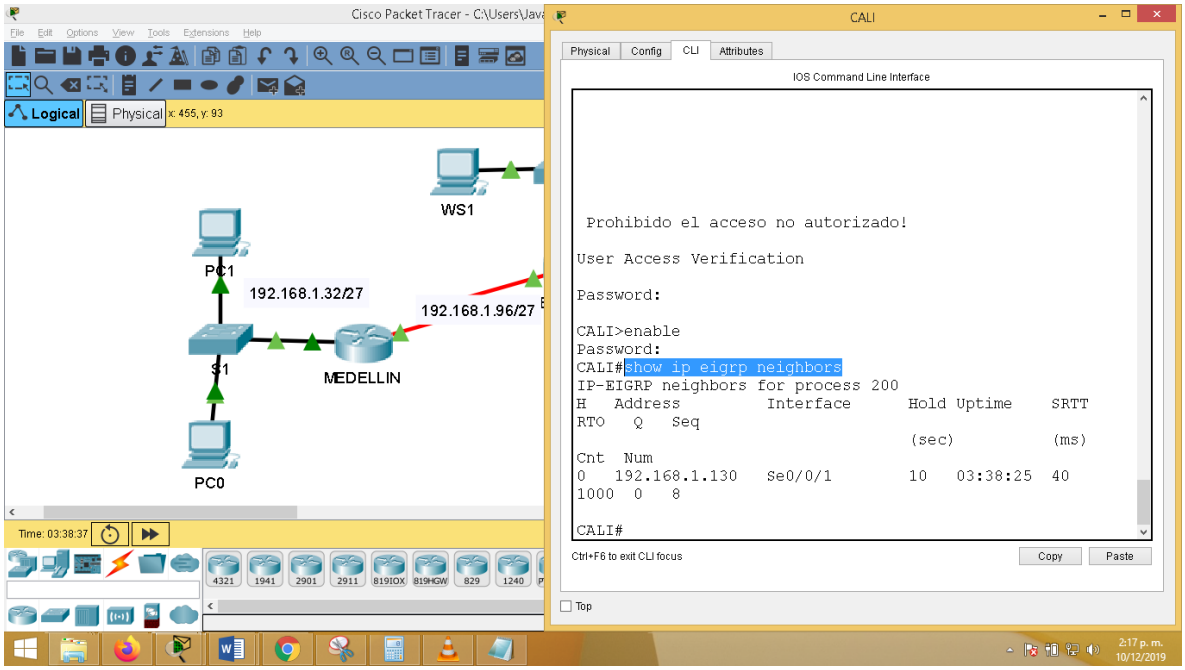
De tal modo que se puede verificar que hay dos vecindades:

Interfaz Serial 0/0/0 con dirección IP 192.168.1.99 → pertenece al roture Medellín

Interfaz Serial 0/0/1 con dirección IP 192.168.1.131→ pertenece al roture Cali

Verificando vecindad EIGRP en router Cali

Figura 28. Vecindad EIGRP router Cali



Fuente 34. prueba de habilidades prácticas, Autor: Javier Bulla

Para finalizar se verifica la vecindad en el router Cali, de tal manera que se pueda verificar el del mismo, para ello se ejecuta el comando:

CALI#show ip eigrp neighbors

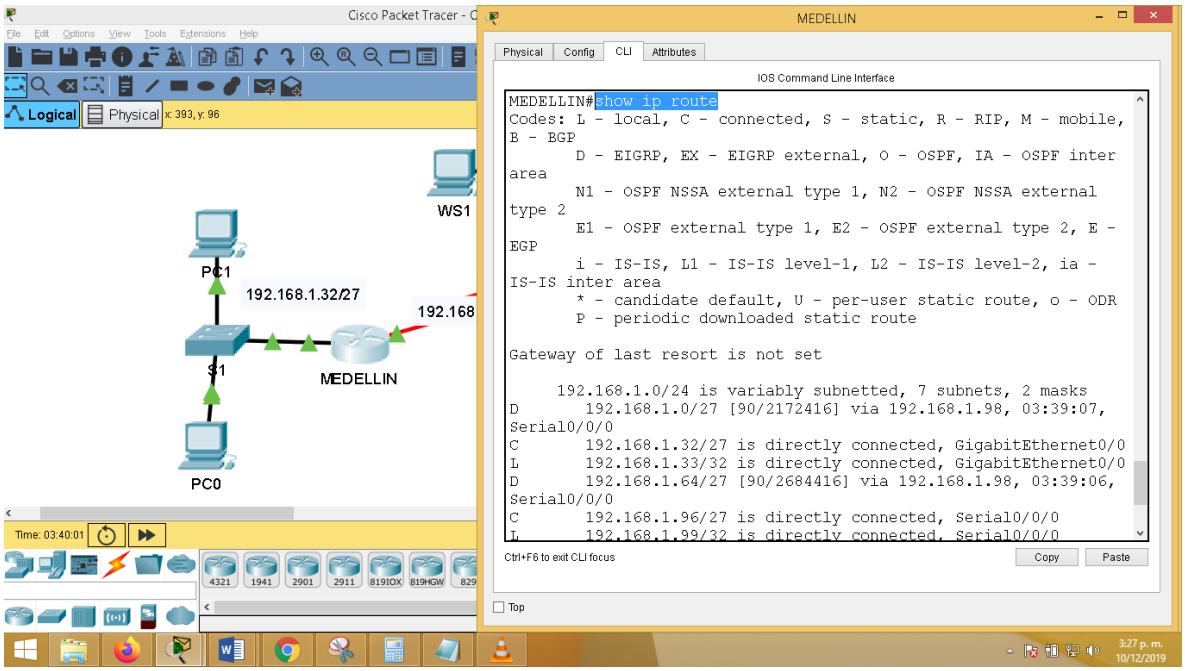
De tal modo que se puede ver, que existe una vecindad:

En la Interfaz serial 0/0/1 con dirección IP 192.168.1.130 → la cual pertenece al router Bogotá.

4.1.3.3 Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

Tabla de enrutamiento en router Medellín

Figura 29.Tabla de enrutamiento de router Medellín



Fuente 35. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar las rutas que están configuradas en el router se ejecutan dos comandos.

MEDELLIN#show ip route

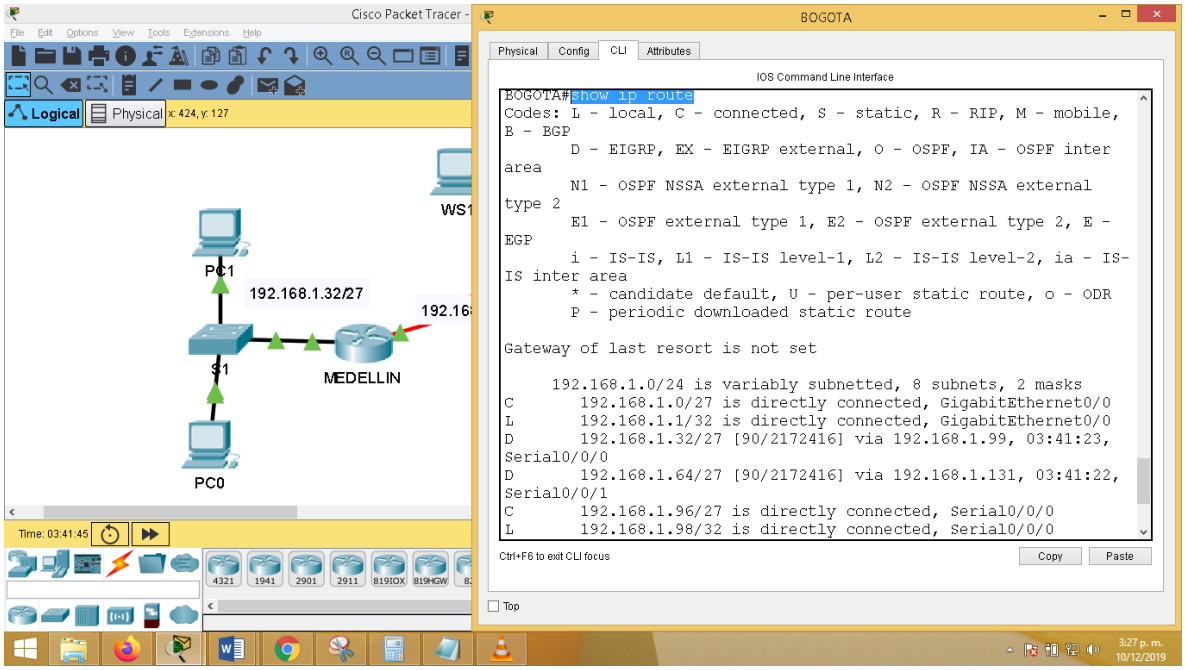
Permite verificar las direcciones que están configuradas en el router.

MEDELLIN#show arp

Permite verificar las direcciones que están en la tabla de enrutamiento en el router.

Tabla de enrutamiento en router Bogotá

Figura 30. Tabla de enrutamiento de router Medellín



Fuente 36. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo, se verifica que la tabla de enrutamiento en el router Bogotá, para ello se ejecuta el comando:

BOGOTA#show ip route

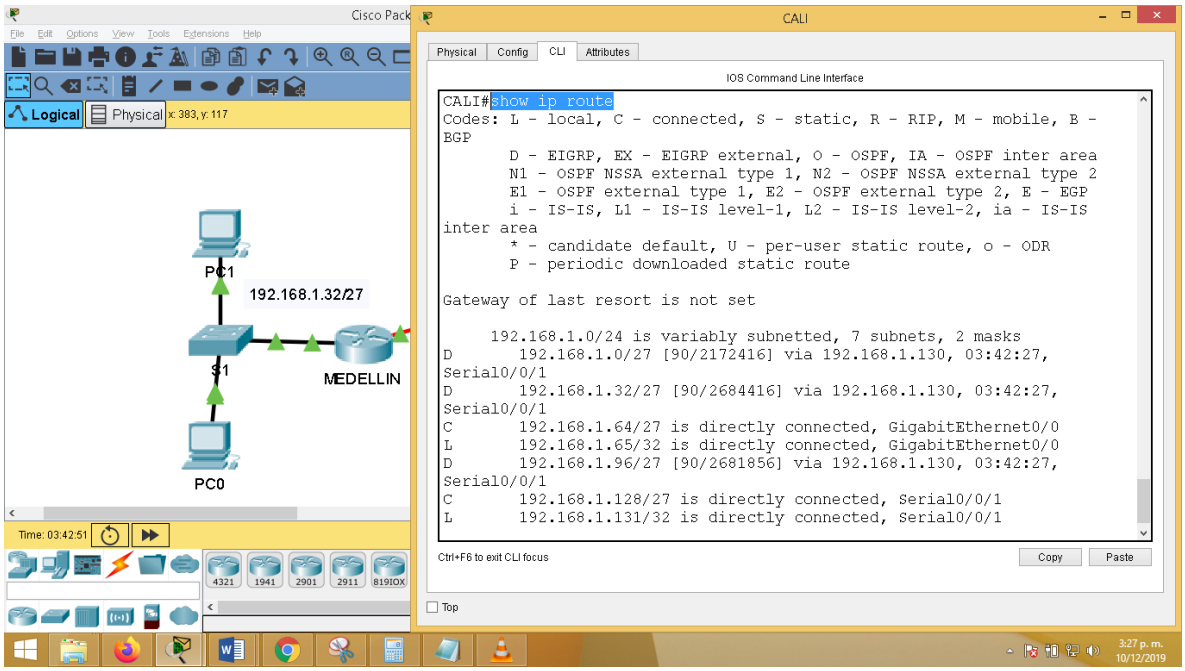
Tambien se ejecuta el comando:

BOGOTA#show arp

Para verificar la tabla de enrutamiento.

Tabla de enrutamiento en router Cali

Figura 31. Tabla de enrutamiento de router Cali



Fuente 37. prueba de habilidades prácticas, Autor: Javier Bulla

Para finalizar se verificar la tabla de enrutamiento en el router Cali, para tal efecto se ejecuta el comando:

CALI#show ip route

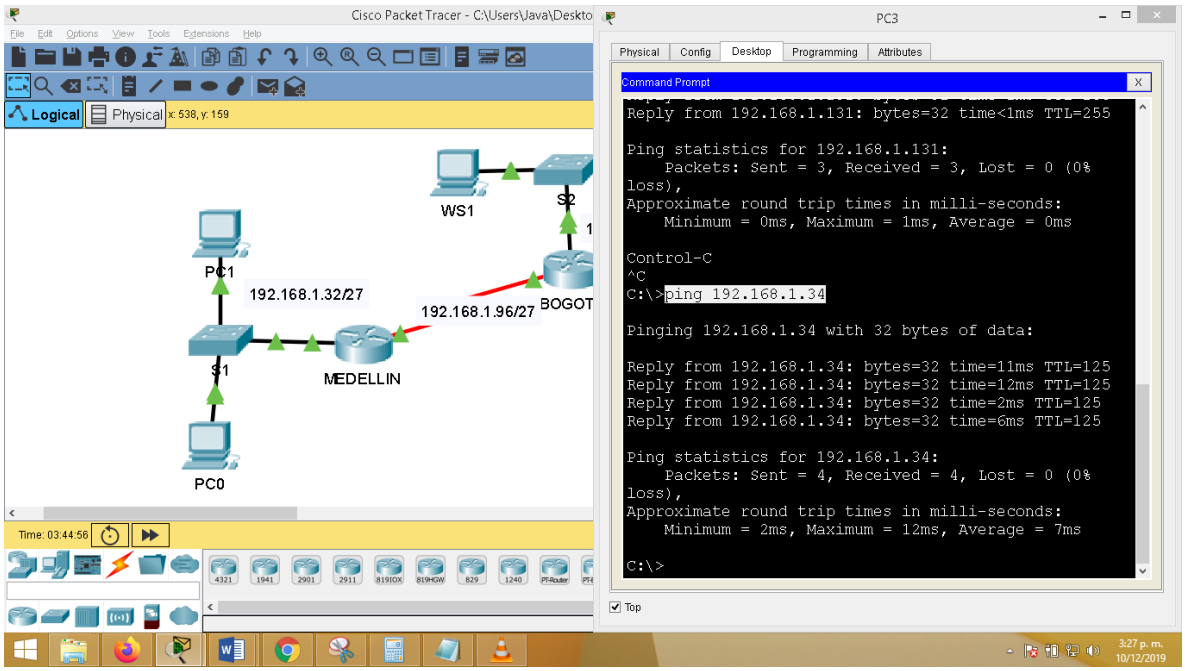
De igual modo se ejecuta el comando:

CALI#show arp

4.1.3.4 Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

Ping de PC3, perteneciente a subred de Cali a PC1 perteneciente a subred Medellín.

Figura 32.Verificando conexión de pc3 de la subred Cali a otros dispositivos.



Fuente 38. prueba de habilidades prácticas, Autor: Javier Bulla

Se procede a verificar conectividad de PC3, el cual pertenece a la subred de CALI, a el PC1 que pertenece a la subred de Medellín.

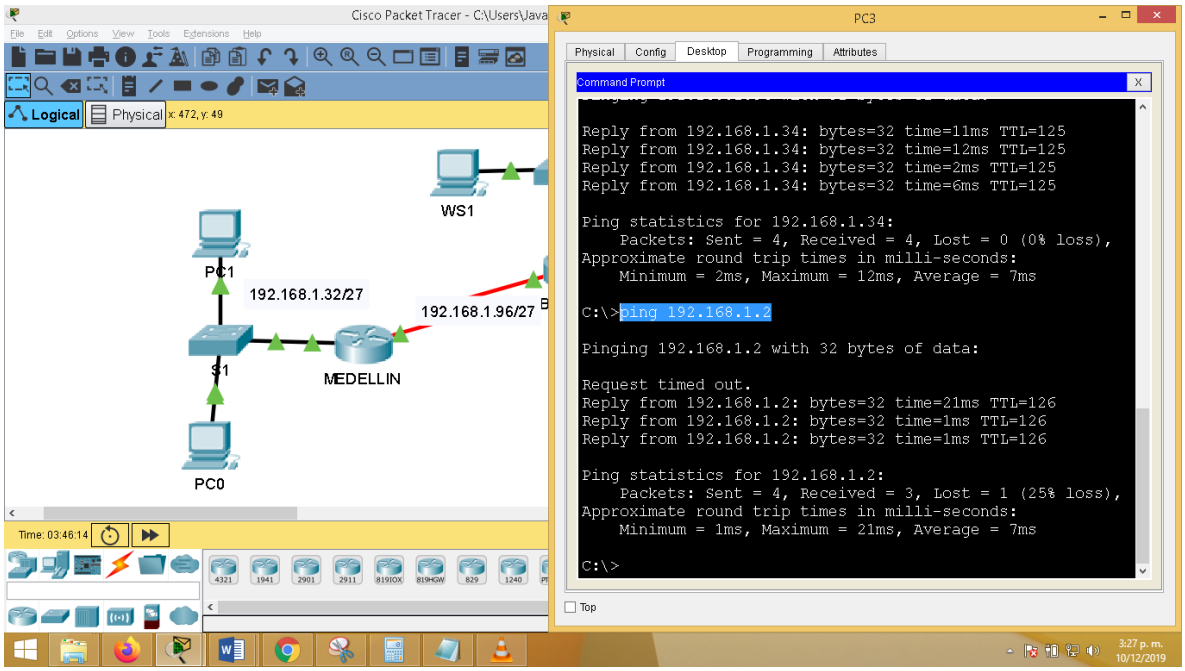
Se puede verificar que el comando PING, se ejecutó satisfactoriamente y que hay conectividad entre los dispositivos.

COMANDO

C:\>ping 192.168.1.34

Ping de PC4, perteneciente a subred de Cali a Servidor que perteneciente a subred Bogotá.

Figura 33. Verificando conexión de pc3 de la subred Cali a otros dispositivos.



Fuente 39. prueba de habilidades prácticas, Autor: Javier Bulla

Se procede a ejecutar el comando ping, del PC4, perteneciente a la subred de Cali a el servidor que se encuentra en la subred de Bogotá.

Se puede verificar que hay conectividad entre los dispositivos.

4.1.4. Parte 4: Configuración de las listas de Control de Acceso.

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo.

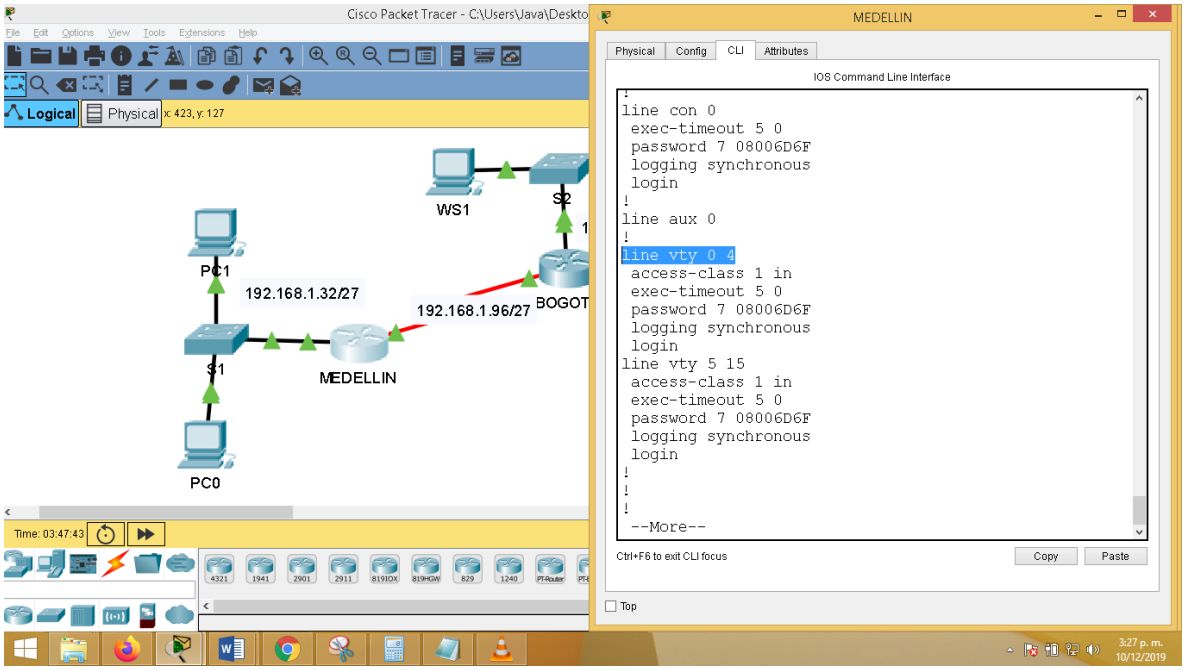
El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

4.1.4.1 Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.

Verificando configuración vty, router Medellín.

Figura 34. Verificando configuracion vty, para acceso remoto en dispositivo Medellin



Fuente 40. prueba de habilidades prácticas, Autor: Javier Bulla

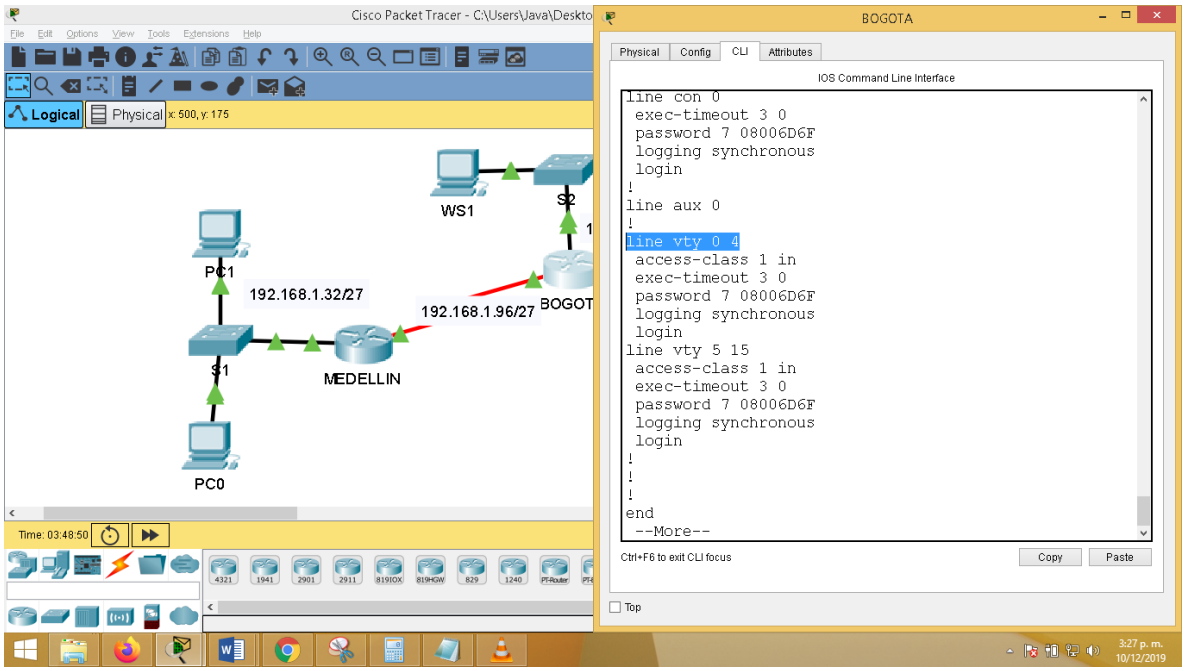
Se puede verificar que la configuración telnet está habitada, puesto que fue realizada, dicha en las configuraciones básicas, de igual modo no se repetirá dicho proceso.

Para verificar que la configuración esta implementada con éxito se ejecuta el comando:

BOGOTA#show run

Verificando configuración vty ., router Bogotá

Figura 35. Verificando configuración vty, para acceso remoto en dispositivo Bogotá



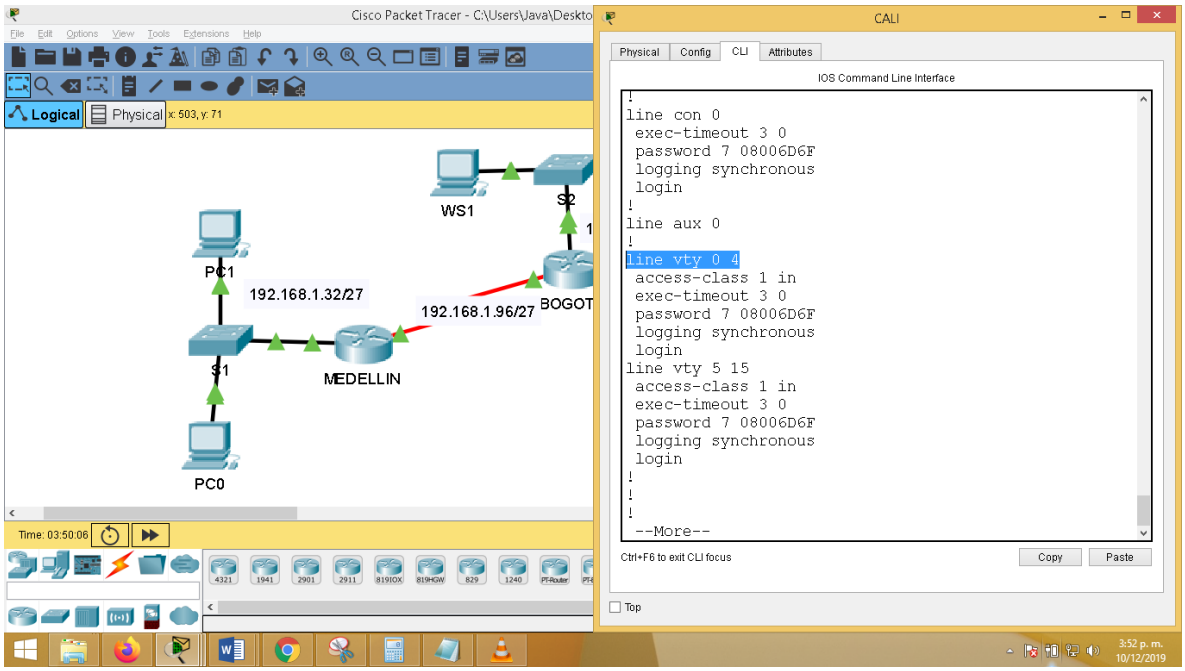
Fuente 41. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar que la configuración esta implementada con éxito se ejecuta el comando:

BOGOTA#show run

Verificando configuración vty ., router Cali

Figura 36. Verificando configuración vty, para acceso remoto en dispositivo Cali



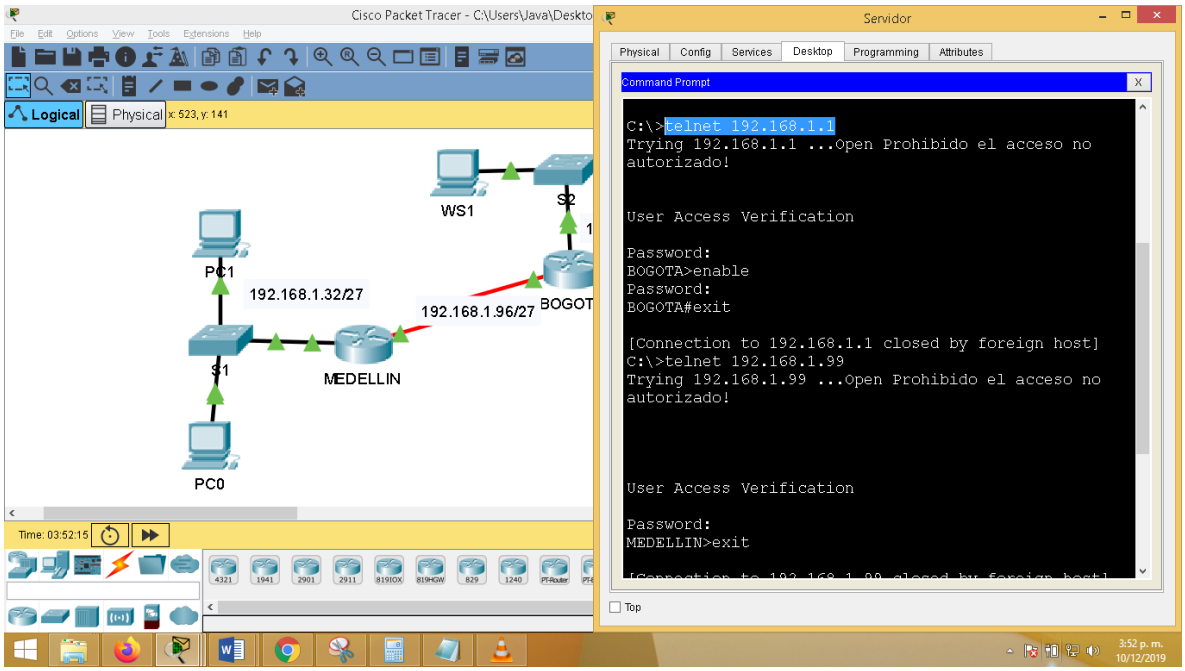
Fuente 42. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar que la configuración esta implementada con éxito se ejecuta el comando:

BOGOTA#show run

Verificando funcionamiento Telnet desde servidor.

Figura 37.Verificando acceso a conexión remota en servidor.



Fuente 43. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar el acceso por telnet desde cualquier dispositivo a los diferentes routers, de Bogotá, Medellín, Cali, se ejecutan los siguientes comandos:

C:\>telnet 192.168.1.1 → Dirección IP de interfaz de router Bogotá.

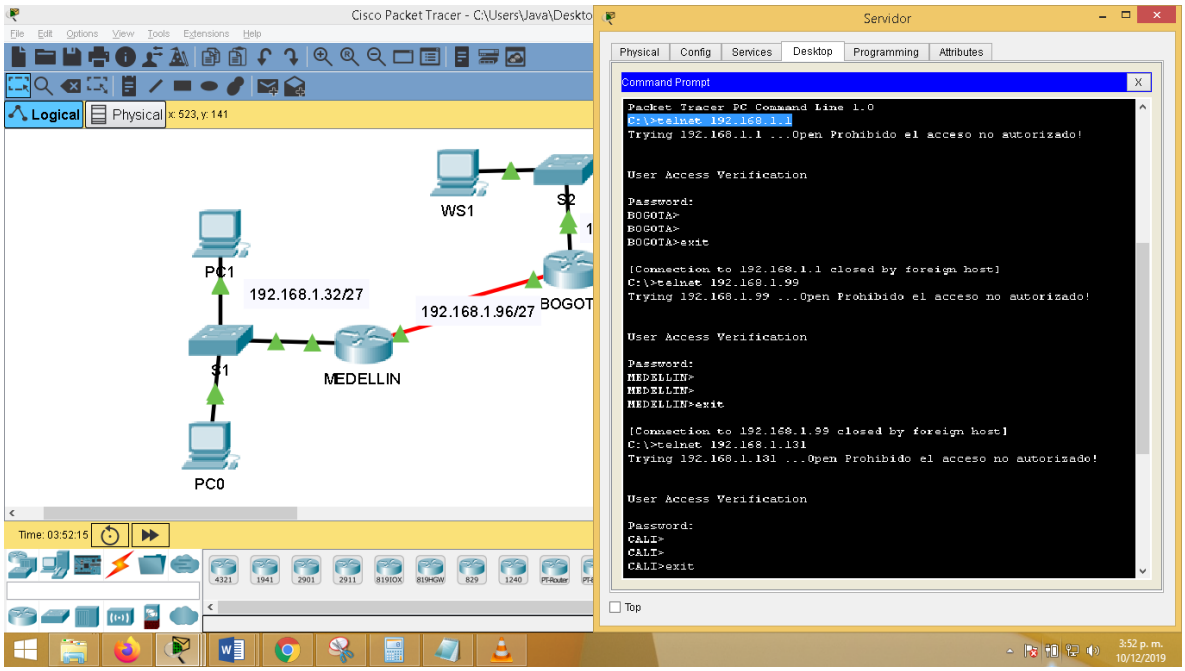
C:\>telnet 192.168.1.99 → Dirección IP de interfaz de router Medellín

C:\>telnet 192.168.1.131 → Dirección IP de interfaz de router Cali.

Se puede verificar que el host Servidor puede acceder de forma remota a cualquier router de la red.

Verificando acceso por telnet desde PC3 a todos los routers de la red.

Figura 38.Verificando acceso telnet a dispositivos routers desde Servidor.



Fuente 44. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo se accede remotamente desde PC3, el cual pertenece a la subred de cali.

C:\>telnet 192.168.1.1 → Dirección IP de interfaz de router Bogotá.

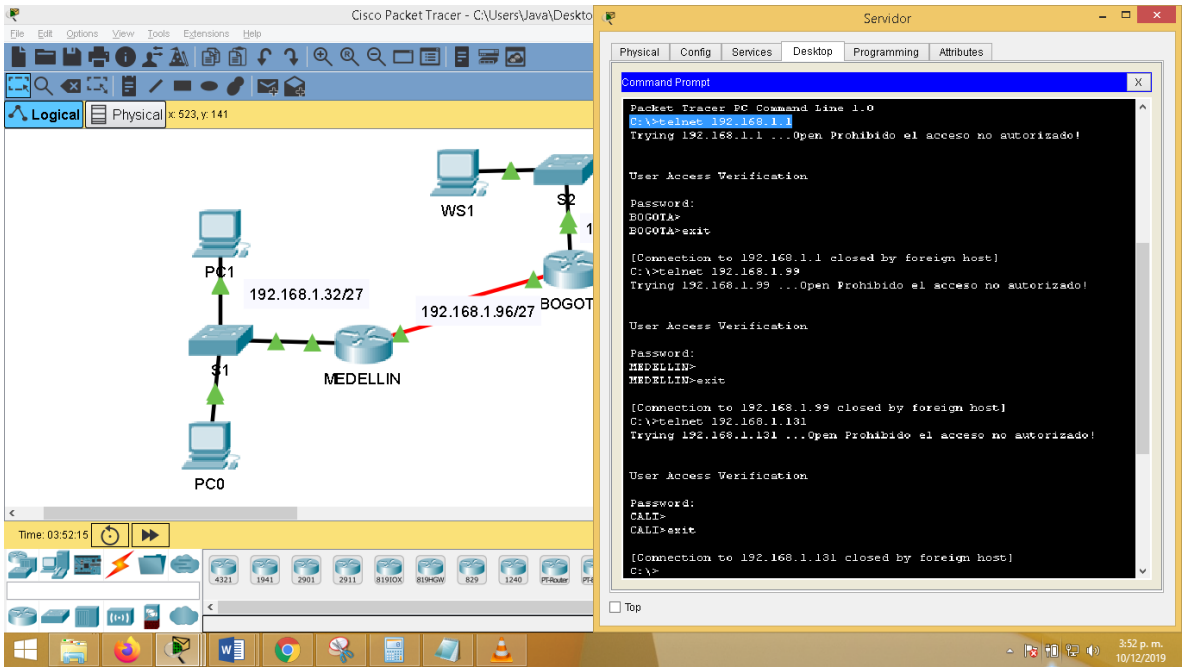
C:\>telnet 192.168.1.99 → Dirección IP de interfaz de router Medellín

C:\>telnet 192.168.1.131 → Dirección IP de interfaz de router Cali.

Se puede verificar que los dispositivos de la subred de Cali pueden acceder remotamente a los routers de la red.

Verificando acceso por telnet desde PC0 a todos los routers de la red.

Figura 39.Verificando acceso via telnet desde servidor.



Fuente 45. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo se verifica que hay acceso remoto desde la PC0 a los routers de la red.

C:\>telnet 192.168.1.1 → Dirección IP de interfaz de router Bogotá.

C:\>telnet 192.168.1.99 → Dirección IP de interfaz de router Medellín

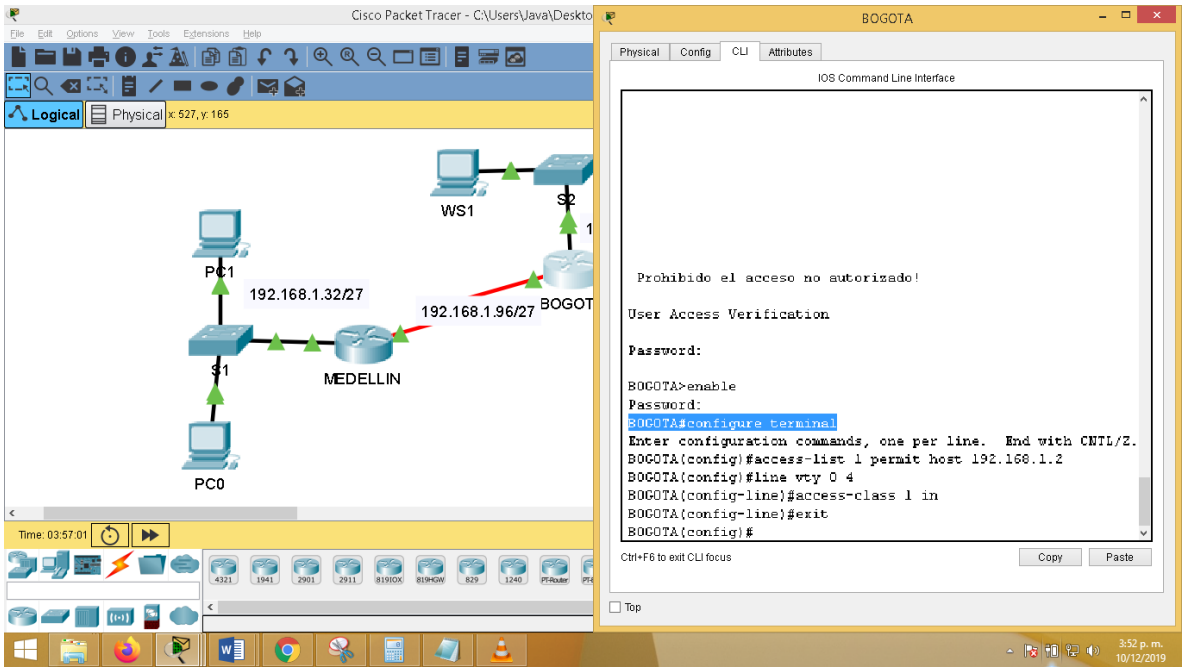
C:\>telnet 192.168.1.131 → Dirección IP de interfaz de router Cali.

Se puede verificar que los dispositivos de la subred de Medellín pueden acceder remotamente a cualquier router de la red por protocolo telnet.

4.1.4.2 El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

Permitiendo acceso remoto solo a servidor de la subred Bogotá.

Figura 40.configurando lista de acceso vty en dispositivo router Bogotá.



Fuente 46. prueba de habilidades prácticas, Autor: Javier Bulla

Para permitir solo el acceso del servidor a cualquier host de la red, se procede a crear una lista de acceso, para ello se ejecuta el siguiente comando:

BOGOTA(config)#access-list 1 permit host 192.168.1.2

En el cual se establece una lista de acceso estándar, que solo permite el acceso al host con la siguiente dirección IP, la cual pertenece a el Servidor.

De igual modo al solo permitir el acceso de un solo host o IP, el router deniega todo por defecto por lo que no hay que especificar más direcciones.

De igual modo se activa la lista de acceso en el protocolo vty, para ello se ejecuta la siguiente línea.

BOGOTA(config)#line vty 0 15

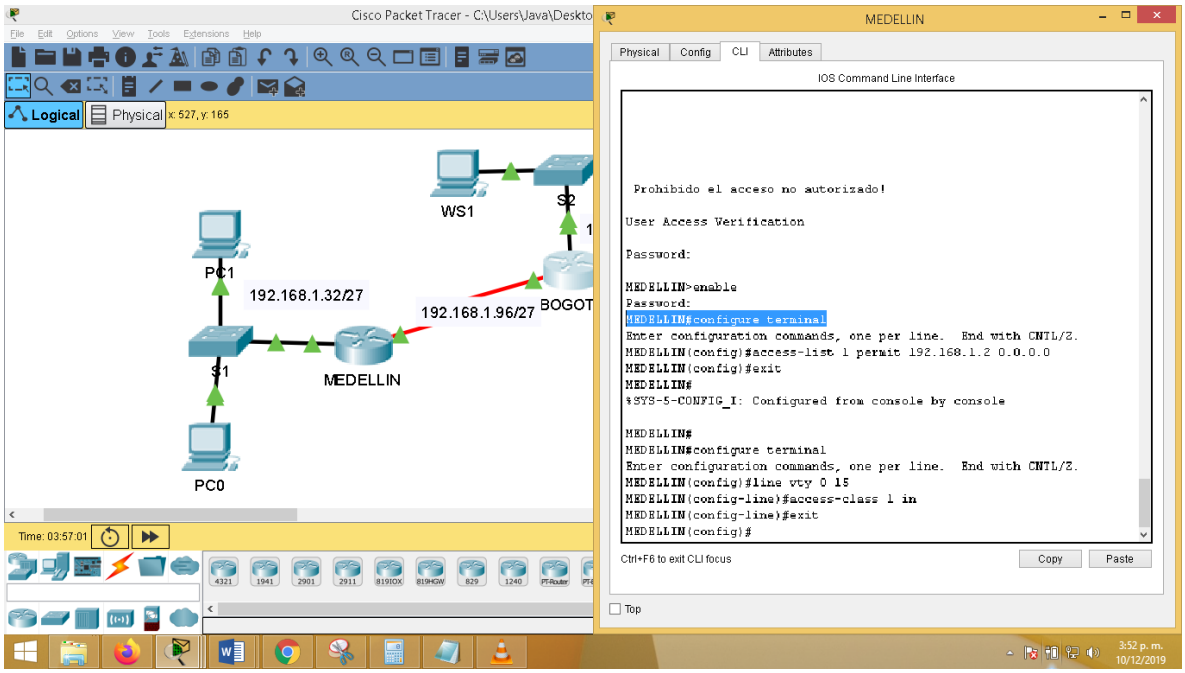
BOGOTA(config-line)#access-class 1 in

BOGOTA(config-line)#exit

De tal modo que el router, solo permitirá el acceso a la lista de acceso 1, la cual solo permite a una, única dirección IP

Permitiendo acceso remoto solo a servidor de la subred Medellín.

Figura 41.configurando lista de acceso vty en dispositivo router Mdellín.



Fuente 47. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo que en el router Bogotá, configuramos el router Medellín, para que este solo permita el acceso remoto a el servidor, para ello se ejecuta los siguientes comandos:

MEDELLIN(config)#access-list 1 permit 192.168.1.2 0.0.0.0

MEDELLIN(config)#exit

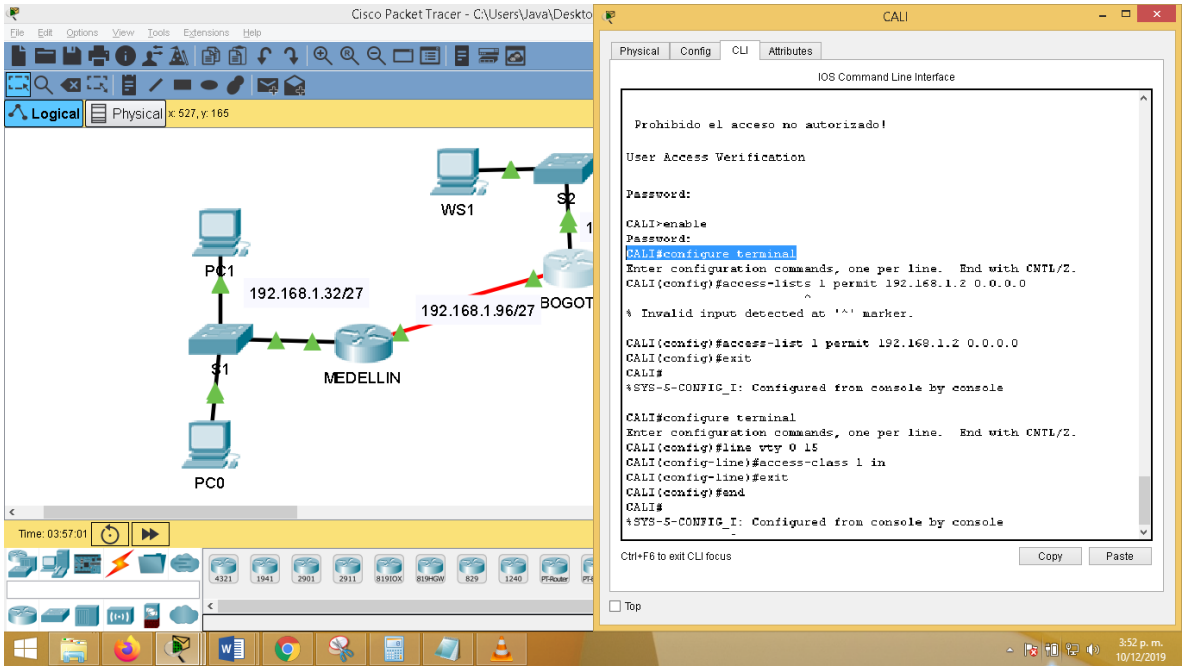
MEDELLIN(config)#line vty 0 15

MEDELLIN(config-line)#access-class 1 in

MEDELLIN(config-line)#exit

Permitiendo acceso remoto solo a servidor de la subred Cali.

Figura 42.configurando lista de acceso vty en dispositivo router Cali.



Fuente 48. prueba de habilidades prácticas, Autor: Javier Bulla

Para finalizar se configura de igual modo, el dispositivo router, para permitir solo acceso a el servidor para ello se ejecutan los siguientes comandos.

CALI(config)#access-list 1 permit 192.168.1.2 0.0.0.0

CALI(config)#line vty 0 15

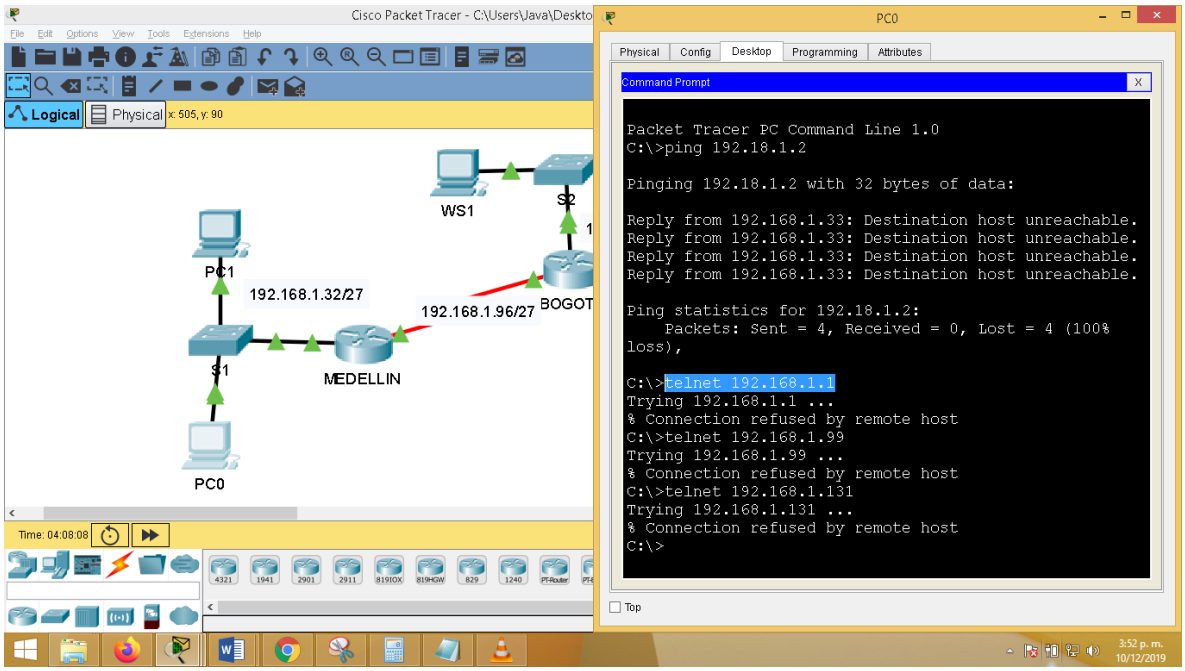
CALI(config-line)#access-class 1 in

CALI(config-line)#exit

4.1.4.3 Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

Verificando acceso telnet desde PC0 de subred Medellín a routers.

Figura 43.verificando acceso remoto por protocolo telnet.



Fuente 49. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la conectividad, se ejecuta nuevamente los siguientes comandos:

C:\>telnet 192.168.1.1 → Resultado sin conexión al router Bogotá

C:\>telnet 192.168.1.99 → Resultado sin conexión al router Medellín

C:\>telnet 192.168.1.131 → Resultado sin conexión al router Cali

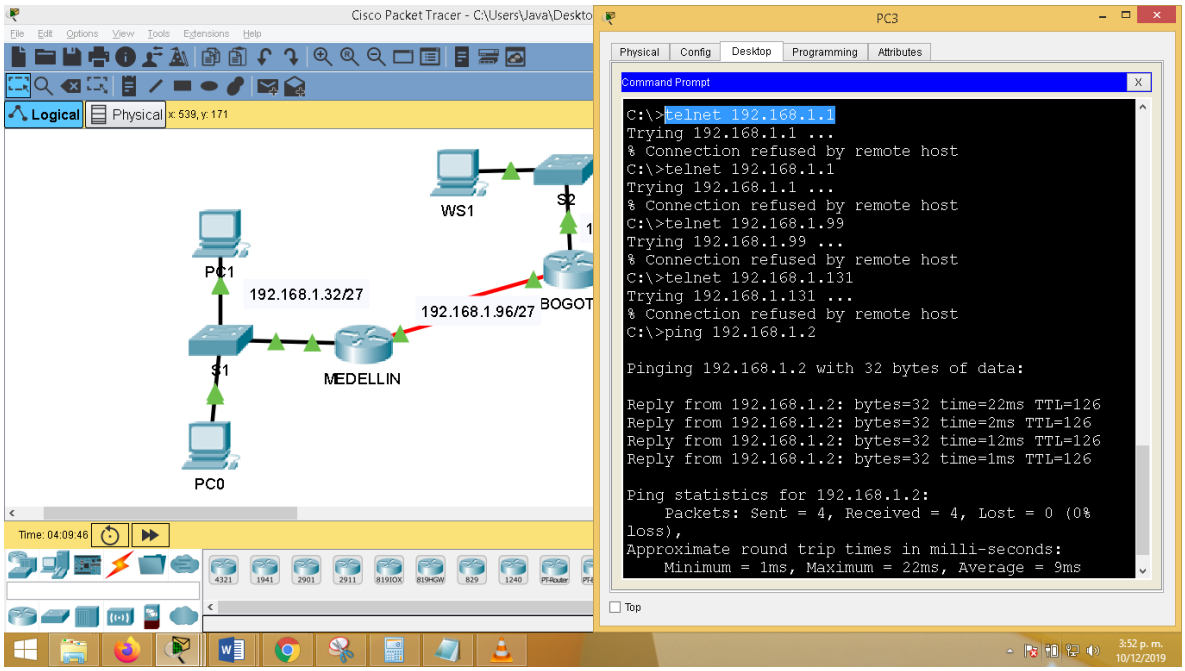
De igual modo se establecerá conexión a el servidor para ello se ejecuta el siguiente comando:

C:\>ping 192.168.1.2 → Resultado satisfactorio hay conexión a servidor.

Se puede verificar que no hay conexión desde ningún dispositivo de la subred Medellín a los routers de la Red.

Verificando acceso telnet desde PC3 de subred Cali a routers.

Figura 44.verificando acceso remoto por protocolo telnet.



Fuente 50. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo se comprobará que no haya acceso telnet a ningún dispositivo de la subred Cali, para tal efecto se ejecuta los siguientes comandos:

C:\>telnet 192.168.1.1 → Resultado sin conexión al router Bogotá

C:\>telnet 192.168.1.99 → Resultado sin conexión al router Medellín

C:\>telnet 192.168.1.131 → Resultado sin conexión al router Cali

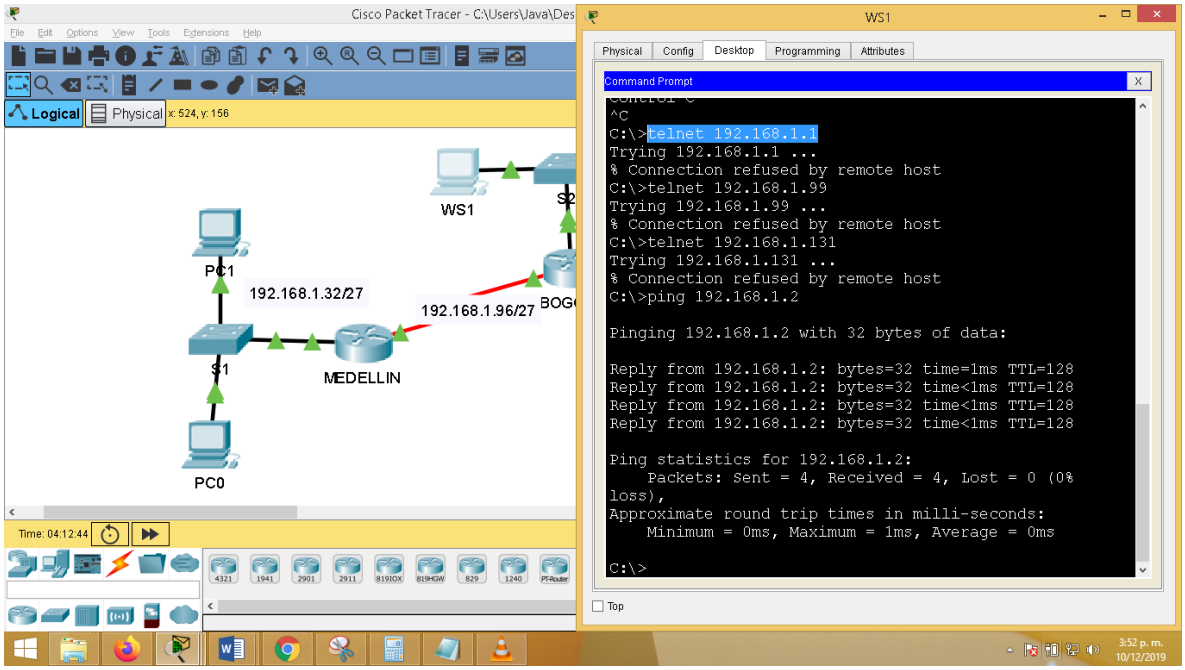
De igual modo se establecerá conexión a el servidor para ello se ejecuta el siguiente comando:

C:\>ping 192.168.1.2 → Resultado satisfactorio hay conexión a servidor.

Se puede verificar que no hay conexión desde ningún dispositivo de la subred Cali a los routers de la Red.

Verificando acceso telnet desde WS1 de subred Bogotá a routers.

Figura 45. verificando acceso remoto por protocolo telnet.



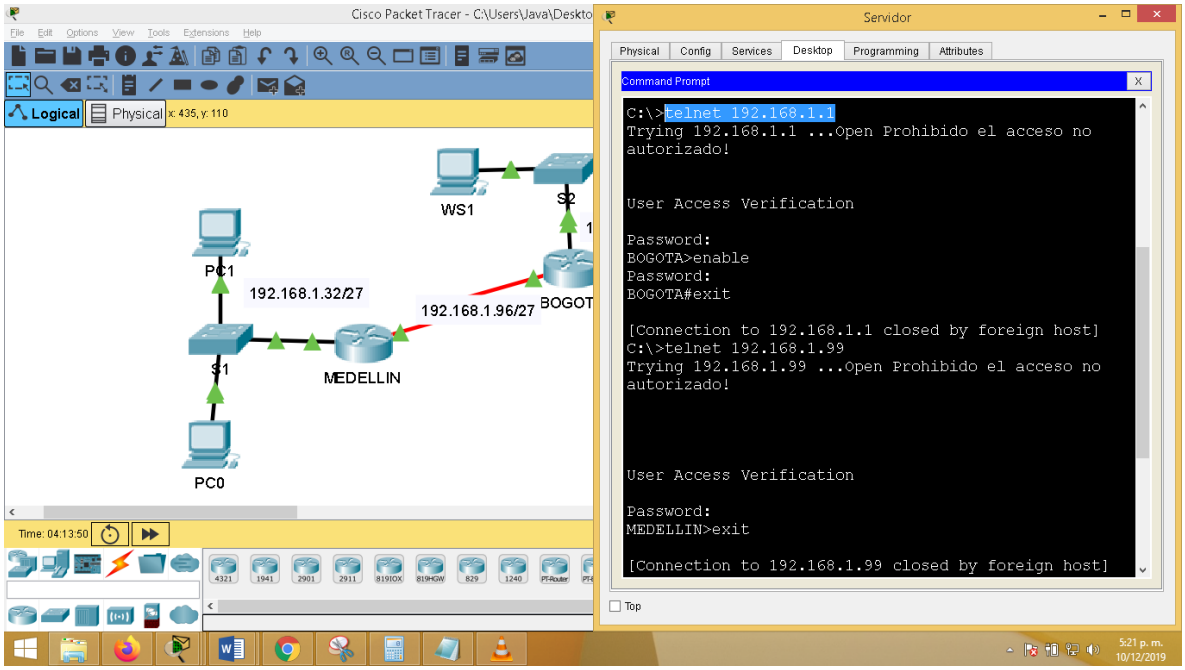
Fuente 51. prueba de habilidades prácticas, Autor: Javier Bulla

Se puede verificar que tampoco se le es permitido el acceso telnet a el dispositivo WS1, aunque pertenece a la subred de Bogotá la misma del Servidor.

Aunque de igual modo establece comunicación exitosa con el servidor.

Verificando acceso telnet desde el servidor de subred Bogotá a routers.

Figura 46. verificando acceso remoto por protocolo telnet.



Fuente 52. prueba de habilidades prácticas, Autor: Javier Bulla

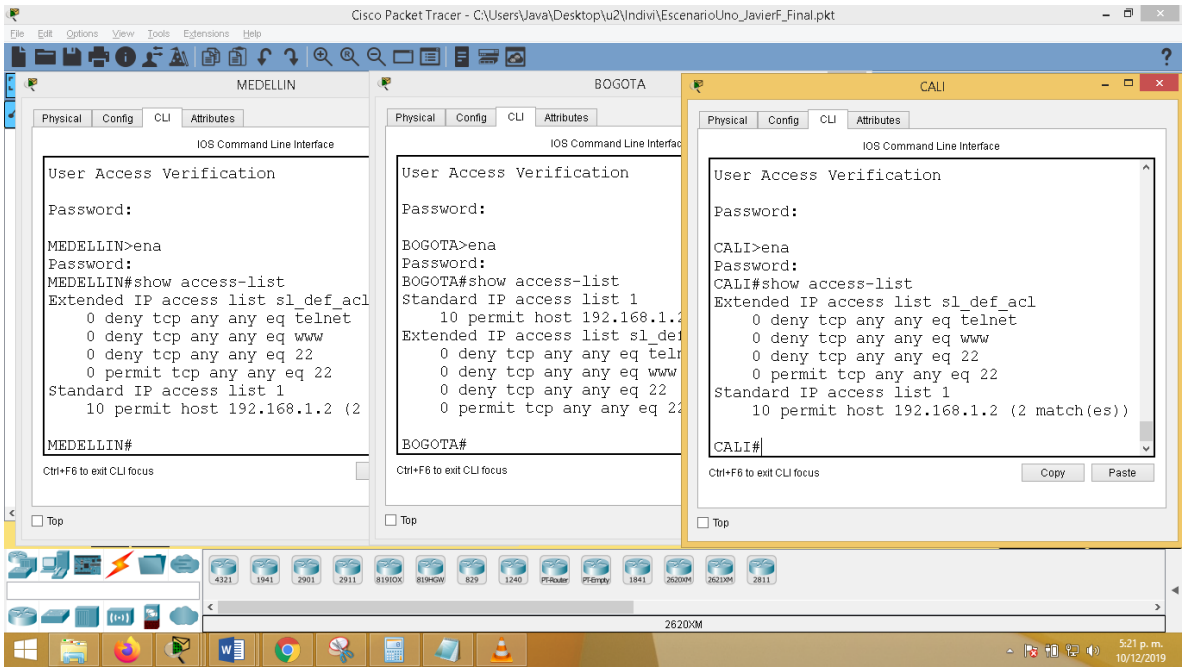
Se puede verificar que hay conexión exitosa del servidor a cualquier dispositivo de la red.

4.1.5. Parte 5: Comprobación de la red instalada.

4.1.5.1 Se debe probar que la configuración de las listas de acceso fue exitosa.

Verificando éxito de lista de acceso

Figura 47.verificando listas de acceso en dispositivos capa tres routers.



Fuente 53. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar el éxito de la lista de acceso, se ejecuta el siguiente comando en cada router.

MEDELLIN#show access-list

CALI#show access-list

BOGOTA#show access-list

Se evidencia que sea ejecutado con éxito dos veces, por el dispositivo que cumple la condición, tener la misma dirección IP, especificada en la lista de acceso.

4.1.5.2 Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red.

Tabla 7.Lista de chequeo de resultados y funcionabilidad en la implementación del escenario Uno.

	ORIGEN	DESTINO	RESULTADO

TELNET	Router MEDELLIN	Router CALI	Optimo, según solicitado
	WS_1	Router BOGOTA	Optimo, según solicitado
	Servidor	Router CALI	Optimo, según solicitado
	Servidor	Router MEDELLIN	Optimo, según solicitado
TELNET	LAN del Router MEDELLIN	Router CALI	Optimo, según solicitado
	LAN del Router CALI	Router CALI	Optimo, según solicitado
	LAN del Router MEDELLIN	Router MEDELLIN	Optimo, según solicitado
	LAN del Router CALI	Router MEDELLIN	Optimo, según solicitado
PING	LAN del Router CALI	WS_1	Optimo, según solicitado
	LAN del Router MEDELLIN	WS_1	Optimo, según solicitado
	LAN del Router MEDELLIN	LAN del Router CALI	Optimo, según solicitado
PING	LAN del Router CALI	Servidor	Optimo, según solicitado

	LAN del Router MEDELLIN	Servidor	Optimo, según solicitado
	Servidor	LAN del Router MEDELLIN	Optimo, según solicitado
	Servidor	LAN del Router CALI	Optimo, según solicitado
	Router CALI	LAN del Router MEDELLIN	Optimo, según solicitado
	Router MEDELLIN	LAN del Router CALI	Optimo, según solicitado

Fuente 54. prueba de habilidades prácticas, Autor: Javier Bulla

4.1.6. Parte 6. Nota

4.1.6.1 NOTA

Para acceder a la simulación dirigirse a anexos, donde se encontrará el link, de acceso.

4.2. ESCENARIO 2

Tabla 8. Enrutamiento escenario dos

TABLA DE ENRUTAMIENTO				
BUCARAMANGA				
Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway
Router	Serial 0/0/0	172.31.2.34	255.255.255.252	N/C
	G0/0	DHCP	DHCP	192.31.0.1
	G0/0.10	172.31.0.0	255.255.255.192	192.31.0.1
	G0/0.30	172.31.0.64	255.255.255.192	192.31.0.65
PC0	F0/0	DHCP	DHCP	DHCP
PC1	F0/0	DHCP	DHCP	DHCP
TUNJA				
Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway
Router	Serial 0/0/0 clock	172.31.2.33	255.255.255.252	N/C
	Serial 0/0/1clock	172.31.2.37	255.255.255.252	N/C
	G0/1	209.17.220.1	255.255.255.0	N/C

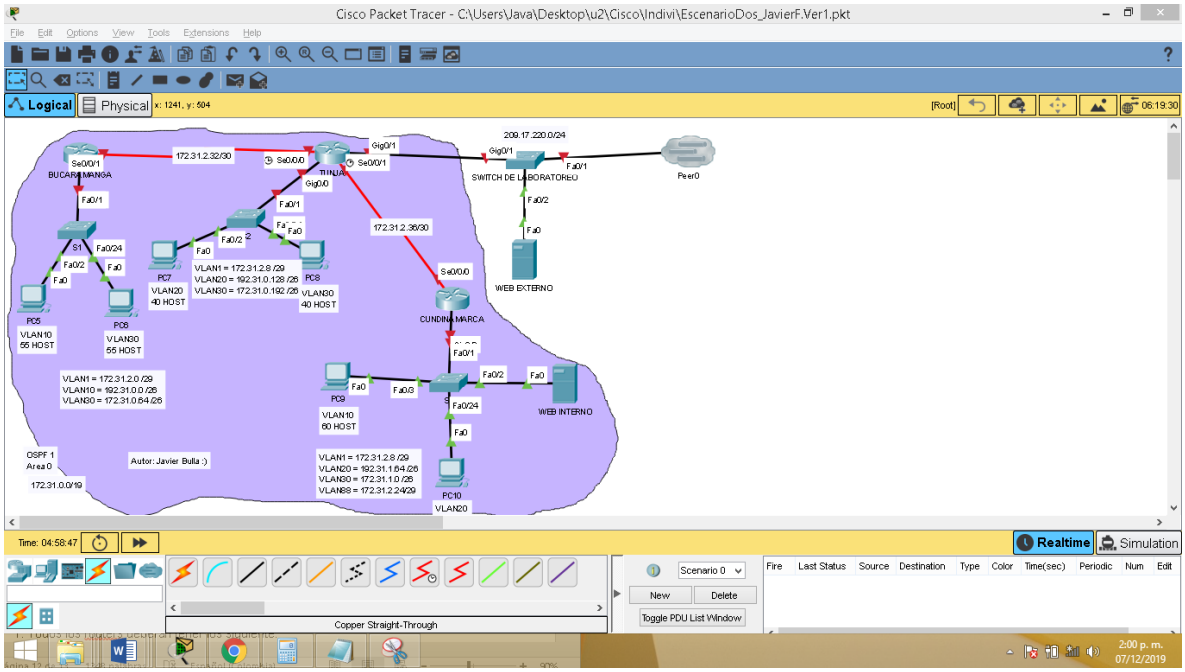
	G0/0	---	---	----
	G0/0.1	172.31.2.9	255.255.255.248	N/C
	G0/0.20	172.31.0.129	255.255.255.192	N/C
	G0/0.30	172.31.0.193	255.255.255.192	N/C
PC7	F0/0	172.31.0.130	255.255.255.192	192.31.0.129
PC8	F0/0	172.31.0.193	255.255.255.192	172.31.0.192
CUNDINAMARCA				
Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway
Router	Serial 0/0/0	172.31.2.38	255.255.255.252	N/C
	G0/0	DHCP	DHCP	N/C
	G0/0.1	172.31.2.8	255.255.255.248	N/C
	G0/0.20	172.31.1.64	255.255.255.192	N/C
	G0/0.30	172.31.1.0	255.255.255.192	N/C
	G0/0.88	172.31.2.25	255.255.255.248	N/C
Servidor TFPT	F0/0	172.31.2.26	DHCP	172.31.2.25
PC9	F0/0	DHCP	DHCP	172.31.1.1
PC10	F0/0	DHCP	DHCP	192.31.1.65
INTERNET				
Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway

Servidor WEB	F0/0	209.17.220.2	255.255.255.0	209.17.220.1

Fuente 55. prueba de habilidades prácticas, Autor: Javier Bulla

La tabla de enrutamiento permite identificar las interfaces de entrada y salida de los dispositivos y las direcciones IP y mascara de red que se asignaran a los hosts.

Figura 48.Topología de red del escenario dos



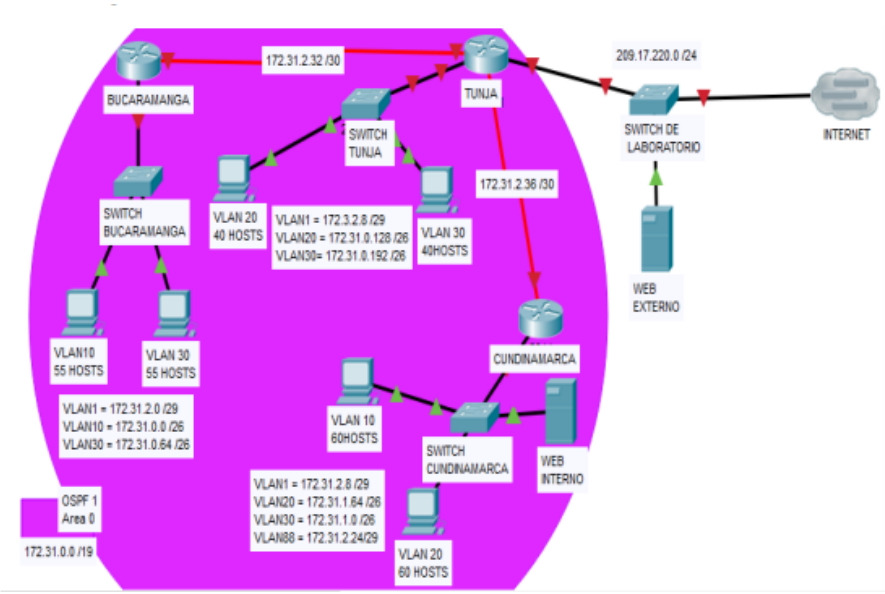
Fuente 56. prueba de habilidades prácticas, Autor: Javier Bulla

Se desarrollará el siguiente escenario dispuesto, para tal efecto se explicará paso a paso el desarrollo del mismo, explicando el procedimiento de forma concisa sin omitir ningún paso llevado a cabo, se evidenciará por medio de imágenes y tablas, acompañadas de una explicación.

La siguiente imagen establece la topología de red, dispuesta para el escenario Dos, para el cual se utilizarán host de tipo, router, Servidor y Computadoras de escritorio.

El desarrollo del mismo se efectuará por medio del software Cisco Packet Tracert, el cual es sugerido para el desarrollo del ejercicio.

Figura 49. Topología de red del escenario dos



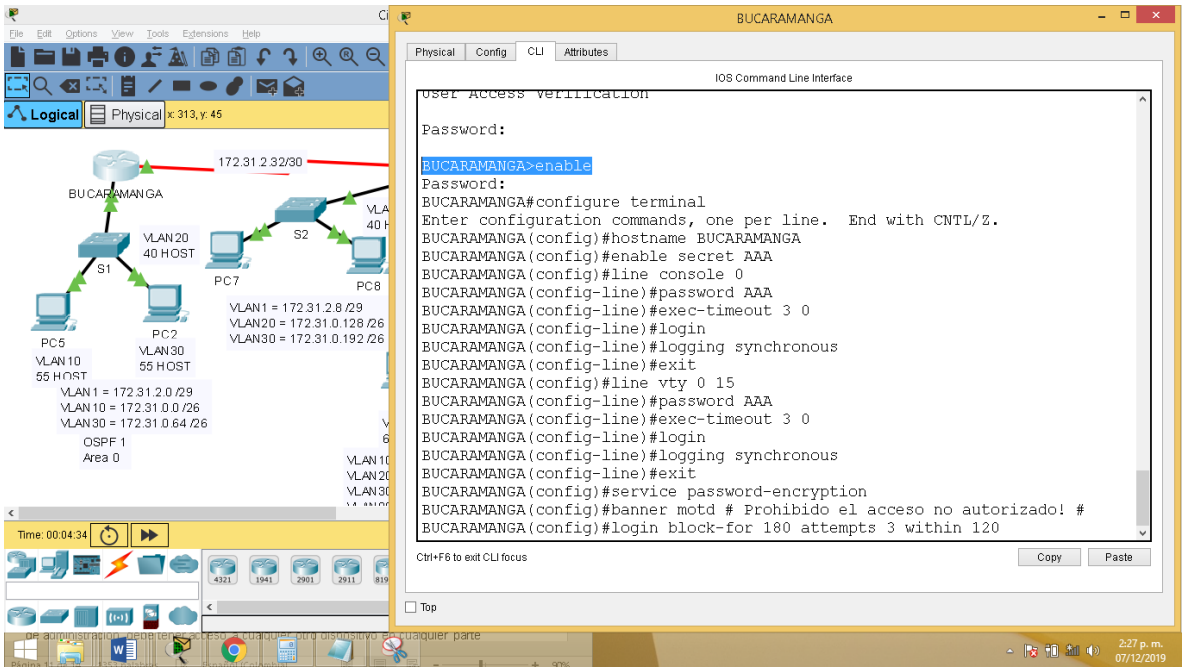
Fuente 57. prueba de habilidades prácticas, Autor: Javier Bulla

Desarrollo.

4.2.1. Parte 1 Todos los routers deberán tener los siguiente:

Configuración router Bucaramanga

Figura 50. Configuración router Bucaramanga



Fuente 58. prueba de habilidades prácticas, Autor: Javier Bulla

Los siguientes comandos se explican a continuación.

4.2.1.1 Configuración básica.

Router(config)#hostname BUCARAMANGA

4.2.1.2 Autenticación local con AAA.

BUCARAMANGA(config)#enable secret AAA

BUCARAMANGA(config)#line console 0

BUCARAMANGA(config-line)#password AAA

BUCARAMANGA(config-line)#exec-timeout 3 0

BUCARAMANGA(config-line)#login

BUCARAMANGA(config-line)#logging synchronous

BUCARAMANGA(config-line)#exit

BUCARAMANGA(config)#line vty 0 15

BUCARAMANGA(config-line)#password AAA

BUCARAMANGA(config-line)#exec-timeout 3 0

BUCARAMANGA(config-line)#login

BUCARAMANGA(config-line)#logging synchronous

BUCARAMANGA(config-line)#exit

4.2.1.3 Cifrado de contraseñas.

BUCARAMANGA(config-line)#service password-encryption

4.2.1.4 Un máximo de internos para acceder al router.

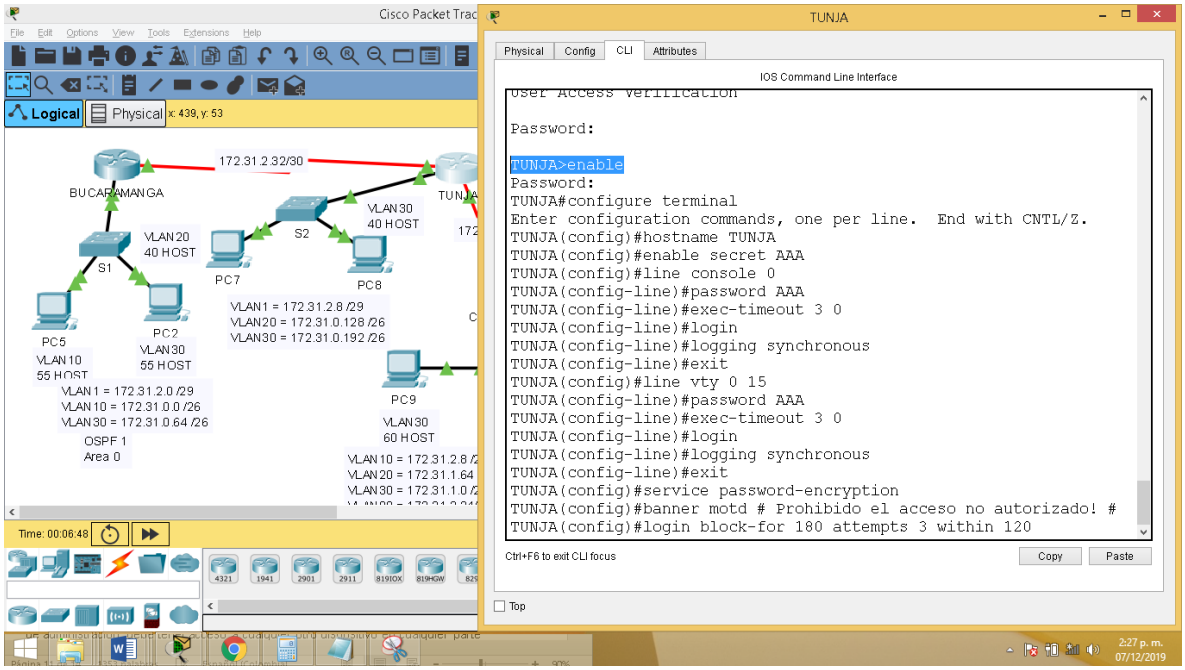
BUCARAMANGA(config)#login block-for 180 attempts 3 within 120

4.2.1.5 Máximo tiempo de acceso al detectar ataques.

BUCARAMANGA(config)#login block-for 180 attempts 3 within 120

Configuracion Bascia Router Tunja

Figura 51. Configuración router Tunja

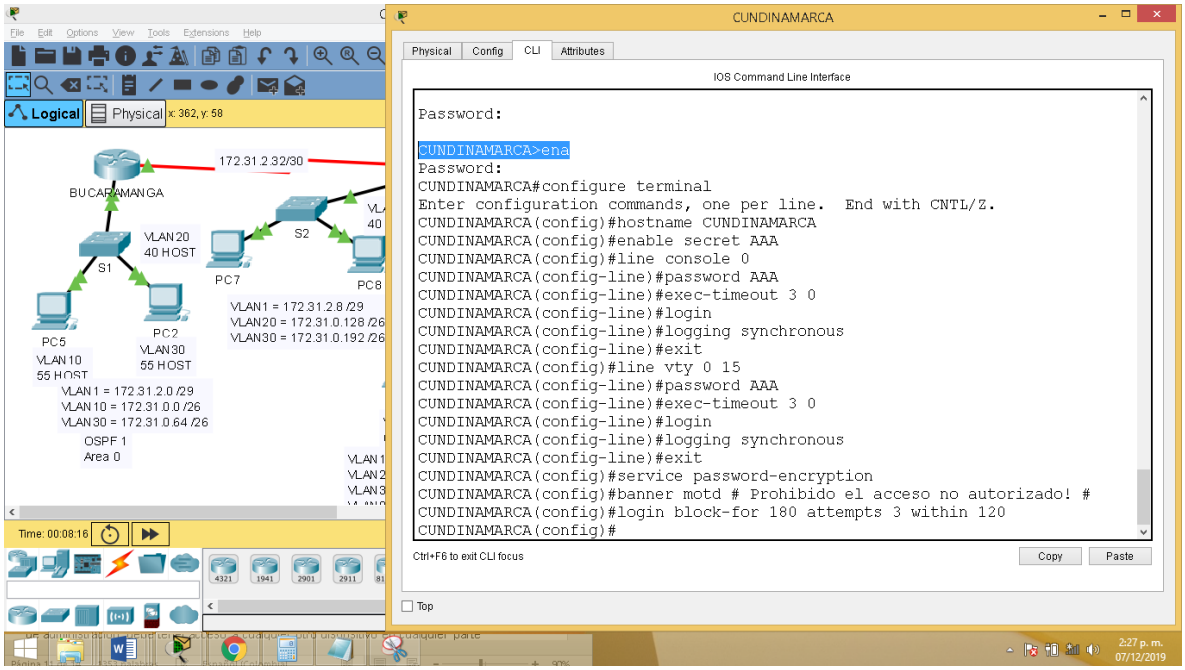


Fuente 59. prueba de habilidades prácticas, Autor: Javier Bulla

Habiendo explicado los comandos en la ilustración 50, se ejecutan los mismos para el router Tunja, teniendo en cuenta algunas variaciones.

Configuración básica Router Cundinamarca

Figura 52. Configuración router Cundinamarca



Fuente 60. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo se realizan las configuraciones para el dispositivo router Cundinamarca, cabe aclarar que también los comandos son los mismos sin embargo se hacen algunas variaciones.

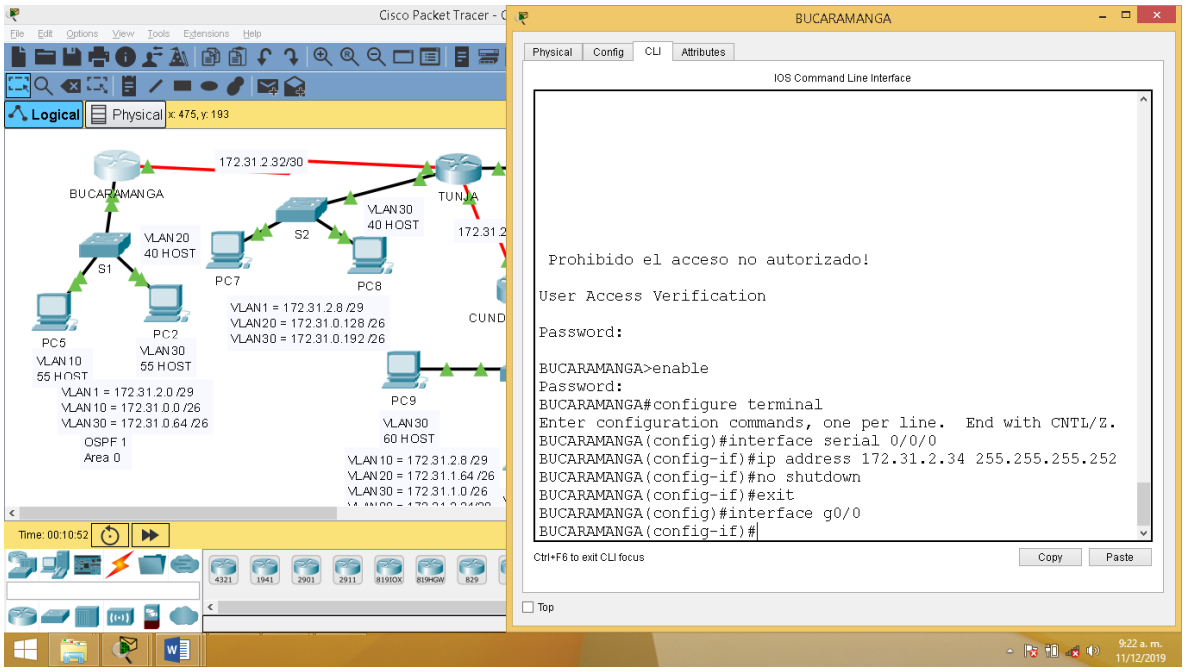
4.2.1.6 Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

Para establecer un servidor TFTP, que almacene todos los archivos de configuración de los routers, se deben configurar sus direcciones IPs, externas.

4.2.2. Parte 2. Configuración de dispositivos de Red.

4.2.2.1 Configuración IP, externa Router Bucaramanga.

Figura 53. Configurando Dirección IP externa Router Bucaramanga



Fuente 61. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar la dirección IP, externa del router Bucaramanga, se ejecutan los siguientes comandos:

Router#configure terminal

BUCARAMANGA(config)#interface serial 0/0/0

BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252

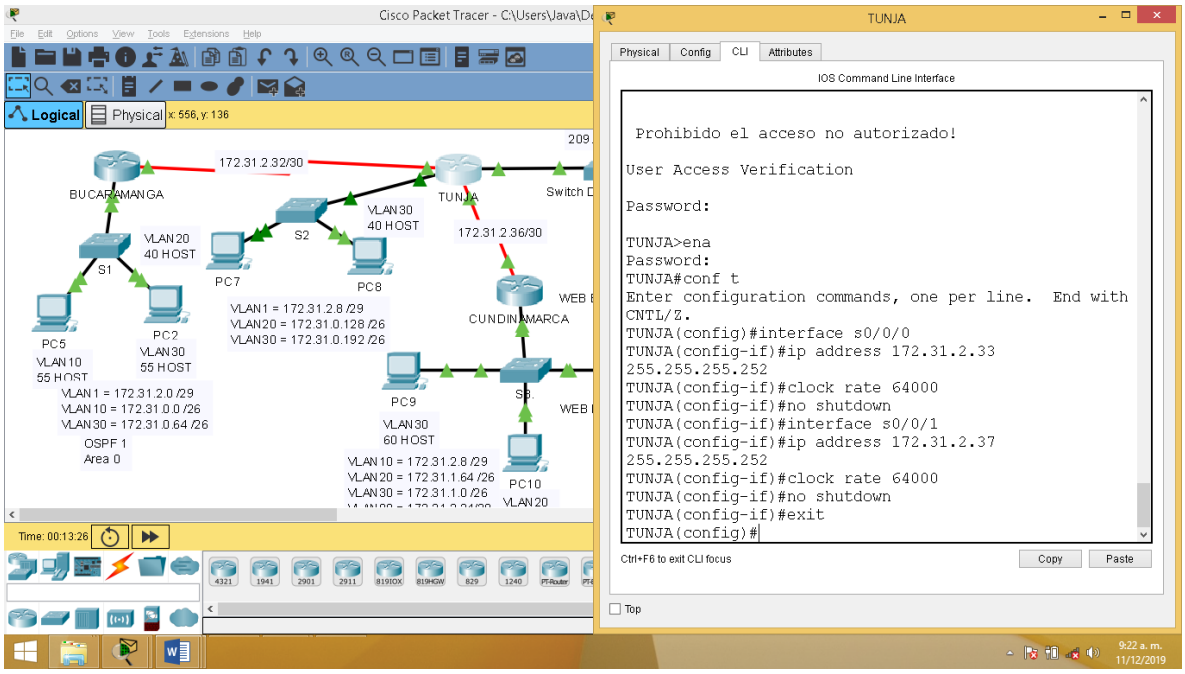
BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#exit

Cabe anotar que solo se está configurando la interface serial 0/0/0, del router Bucaramanga.

4.2.2.2 Configuración IP, externa router Tunja

Figura 54. Configurando Dirección IP externa Router Tunja



Fuente 62. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el router Tunja, se ejecutan lo siguientes comandos:

Configuración para la interface serial 0/0/0

TUNJA(config)#interface s0/0/0

TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252

TUNJA(config-if)#clock rate 64000

TUNJA(config-if)#no shutdown

Configuración para la interface serial 0/0/1

TUNJA(config)#interface s0/0/1

TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252

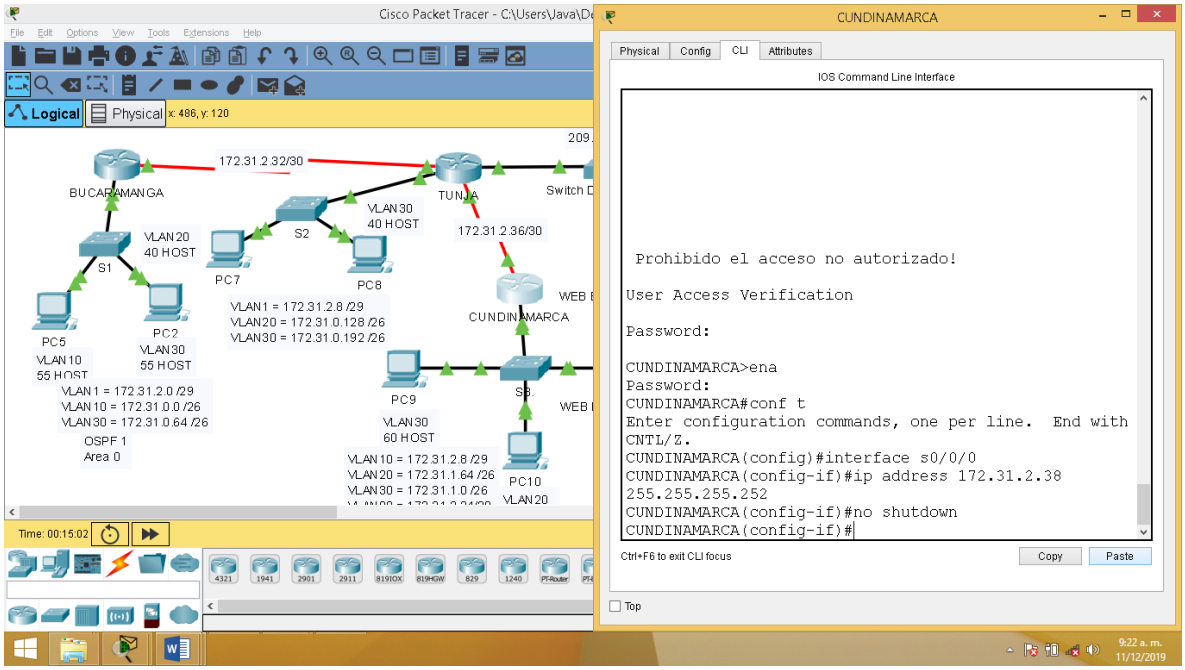
TUNJA(config-if)#clock rate 64000

TUNJA(config-if)#no shutdown

TUNJA(config-if)#exit

4.2.2.3 Configuración IP, externa router Cundinamarca.

Figura 55. Configurando Dirección IP externa Router Cundinamarca



Fuente 63. prueba de habilidades prácticas, Autor: Javier Bulla

Para finalizar se configuración la interfaz de salida del router Cundinamarca, para ello se ejecutan los siguientes comandos:

CUNDINAMARCA(config)#interface s0/0/0

CUNDINAMARCA (config-if)#ip address 172.31.2.38 255.255.255.252

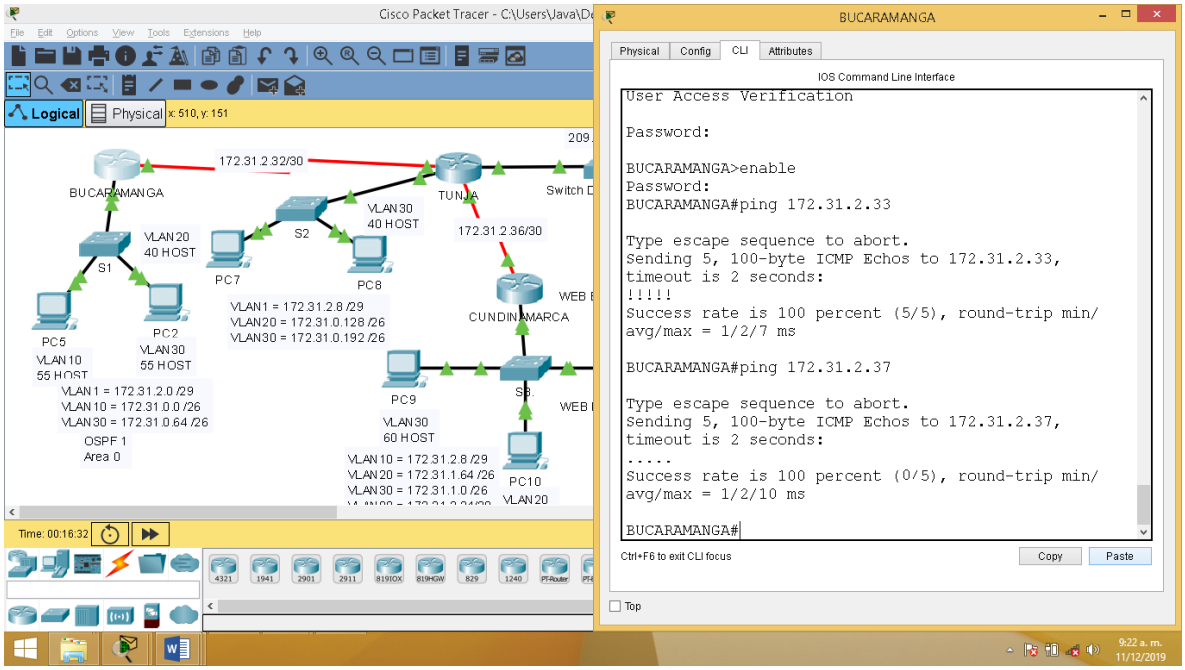
CUNDINAMARCA (config-if)#no shutdown

CUNDINAMARCA (config-if)#exit

4.2.2.4 Verificando conectividad.

Verificando conectividad en router Bucaramanga y Tunja.

Figura 56. Verificando conectividad entre routers



Fuente 64. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la conectividad entre routers, se ejecuta el comando PING:

Se comprobará comunicación en el router Bucaramanga, para ello se ejecuta el comando ping a:

BUCARAMANGA#ping 172.31.2.33 → resultado exitoso, dirección perteneciente a Router Tunja.

BUCARAMANGA#ping 172.31.2.37 → resultado fallido, dirección perteneciente a router Cundinamarca.

Se puede verificar que no hay comunicación con el router de Cundinamarca, esto es debido a que aún no se ha establecido un protocolo de enrutamiento, de tal manera que las subredes de Bucaramanga y Cundinamarca, no se conocen.

Verificando conectividad en router Tunja.

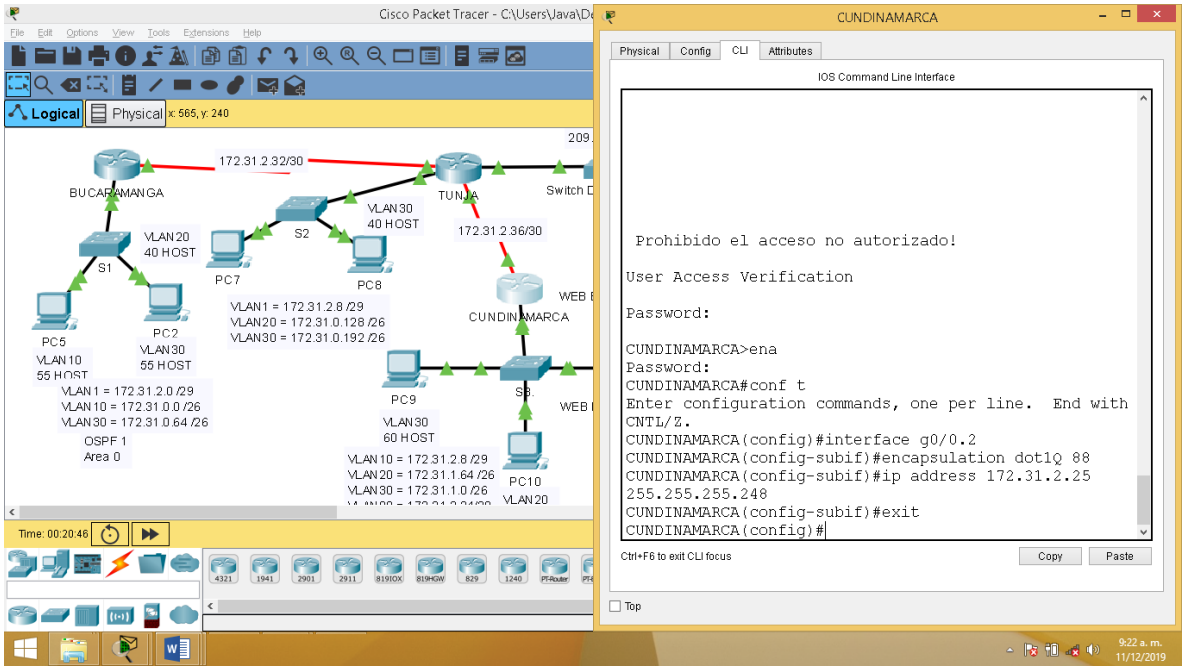
De igual modo en la ilustración 56, se aprecia que también se ejecutó el comando PING:

TUNJA#ping 172.31.2.34 → pertenece a router Bucaramanga, exitoso

TUNJA#ping 172.31.2.38 → pertenece a router Cundinamarca, exitoso

4.2.2.5 Estableciendo Servidor TFTP

Figura 57. Estableciendo servidor TFTP



Fuente 65. prueba de habilidades prácticas, Autor: Javier Bulla

Para establecer el servidor TFTP, se ejecutan los siguientes comandos, cabe anotar que el servidor será asignando a la vlan 88.

Comandos:

CUNDINAMARCA(config-if)#interface g0/0.2

CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248

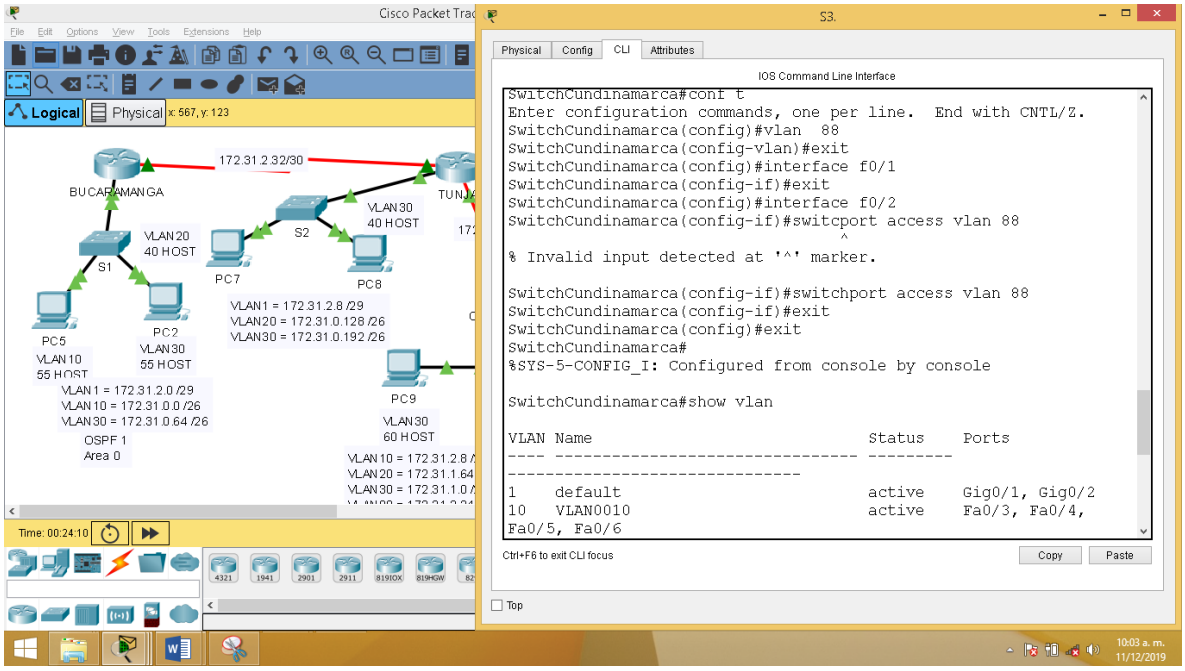
CUNDINAMARCA(config-subif)#encapsulation dot1Q 88

CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248

CUNDINAMARCA(config-subif)#exit

Configurando Vlan 88

Figura 58. creando vlan 88 en dispositivo Switch de la subred Cundinamarca



Fuente 66. prueba de habilidades prácticas, Autor: Javier Bulla

Autor: Javier Felipe Bulla

Para crear la vlan 88 y establecerle un puerto del switch a la misma se ejecutan los siguientes comandos:

SwitchCundinamarca(config)#vlan 88

SwitchCundinamarca(config-if)#exit

SwitchCundinamarca(config)#interface f0/2

SwitchCundinamarca(config-if)#switchport access vlan 88

SwitchCundinamarca(config-if)#exit

De igual modo para verificar que el puerto está asignado correctamente a la vlan se ejecuta el comando.

SwitchCundinamarca#show vlan

SWITCHS CREAR VLANS.

Tabla 9. Tabla de asignación de puertos a vlans, en dispositivos Switchs

CREAR VLANS EN SWITCH BUCARAMANGA	
VLAN	Puertos
Vlan1	g0/1 – g0/2
Vlan10	F0/2 – f0/12
Vlan30	F0/13- f0/24
CREAR VLANS EN SWITCH TUNJA	
VLAN	Puertos
Vlan1	g0/1 – g0/2
Vlan20	F0/6 – f0/16
Vlan30	F0/17- f0/24
CREAR VLANS EN SWITCH CUNDINAMARCA	
VLAN	Puertos
Vlan1	g0/1 – g0/2
Vlan10	F0/2 – F0/7

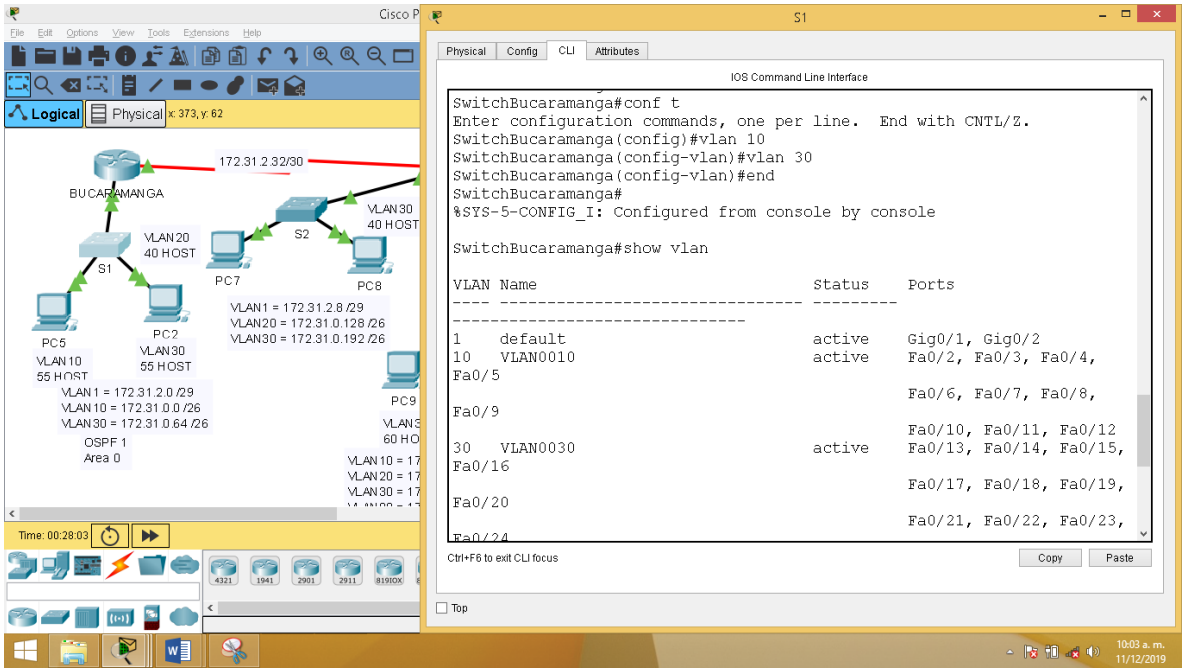
Vlan20	F0/19- F0/24
Vlan30	F0/13- f0/218
Vlan88	F0/8-F0/12

Fuente 67. prueba de habilidades prácticas, Autor: Javier Bulla

4.2.2.6. CONFIGURACION DE SWITCH

4.2.2.6.1 Creando vlans en switchBucaramanga.

Figura 59. Creando vlans en switch Bucaramanga



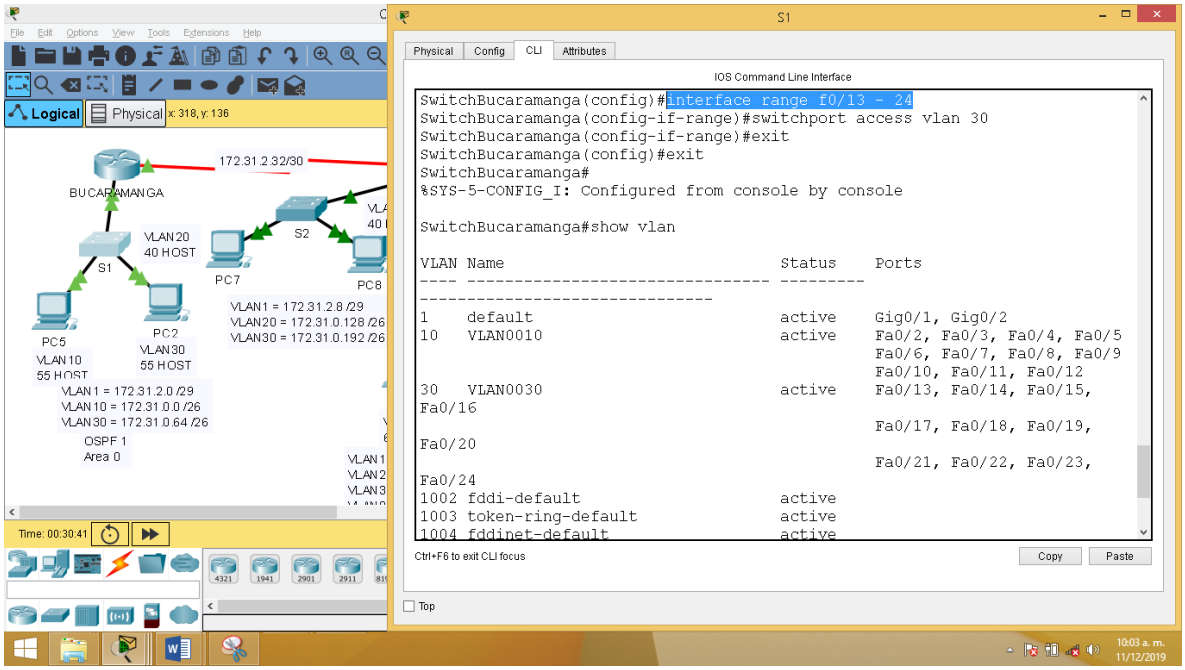
Fuente 68. prueba de habilidades prácticas, Autor: Javier Bulla

Para crear vlans en el switch se ejecuta el comando vlan y el numero en el modo de configuración.

De igual modo para corroborar que fueron creadas exitosamente se ejecuta el comando show vlan.

4.2.2.6.2 Verificando puertos en vlans.

Figura 60. Verificando puertos asignados a vlans



Fuente 69. prueba de habilidades prácticas, Autor: Javier Bulla

Para asignar puertos a una vlan especifica se ejecuta el siguiente comando:

SwitchBucaramanga(config)#*interface range f0/13 - 24*

SwitchBucaramanga(config-if-range)#*switchport access vlan 30*

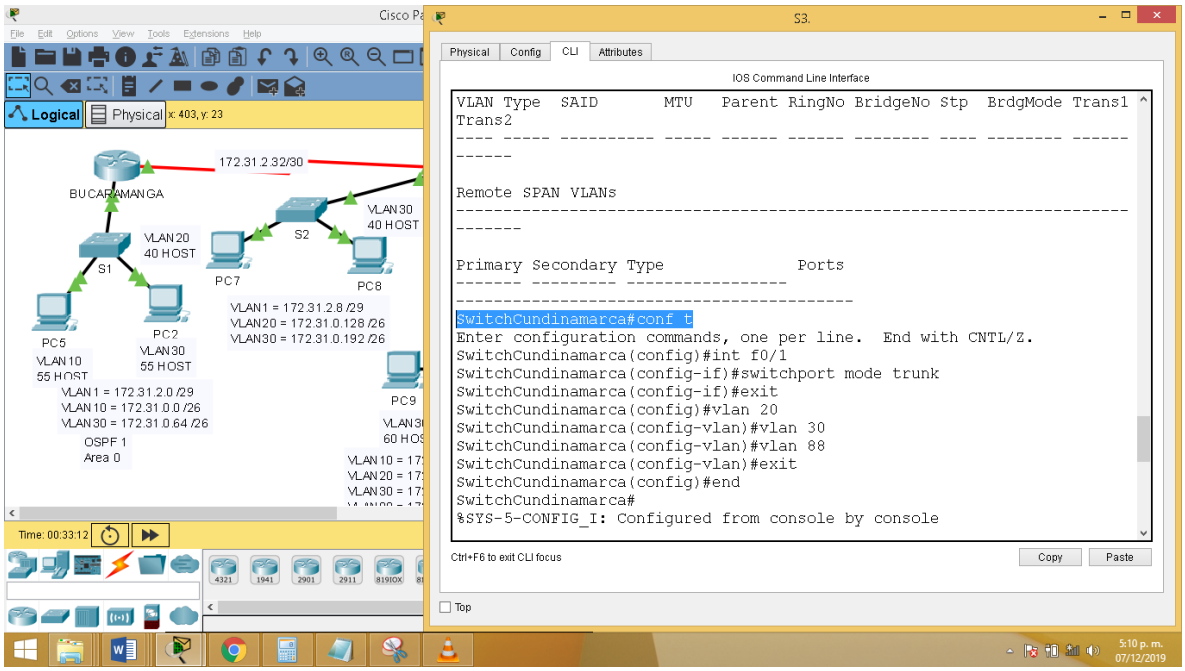
SwitchBucaramanga(config-if-range)#*exit*

De igual modo se procede a verificar su correcta asignación a con el comando show vlan.

SwitchBucaramanga#show vlan

4.2.2.6.3 Creando Vlans en switch Cundinamarca.

Figura 61. Creando vlans en switch Cundinamarca



Fuente 70. prueba de habilidades prácticas, Autor: Javier Bulla

De igual modo que el switch de Bucaramanga, se emplean los mismos comandos para crear vlans en el switch que pertenece a la subred de Cundinamarca.

Comandos:

SwitchCundinamarca(config)#*vlan 20*

SwitchCundinamarca(config-vlan)#*vlan 30*

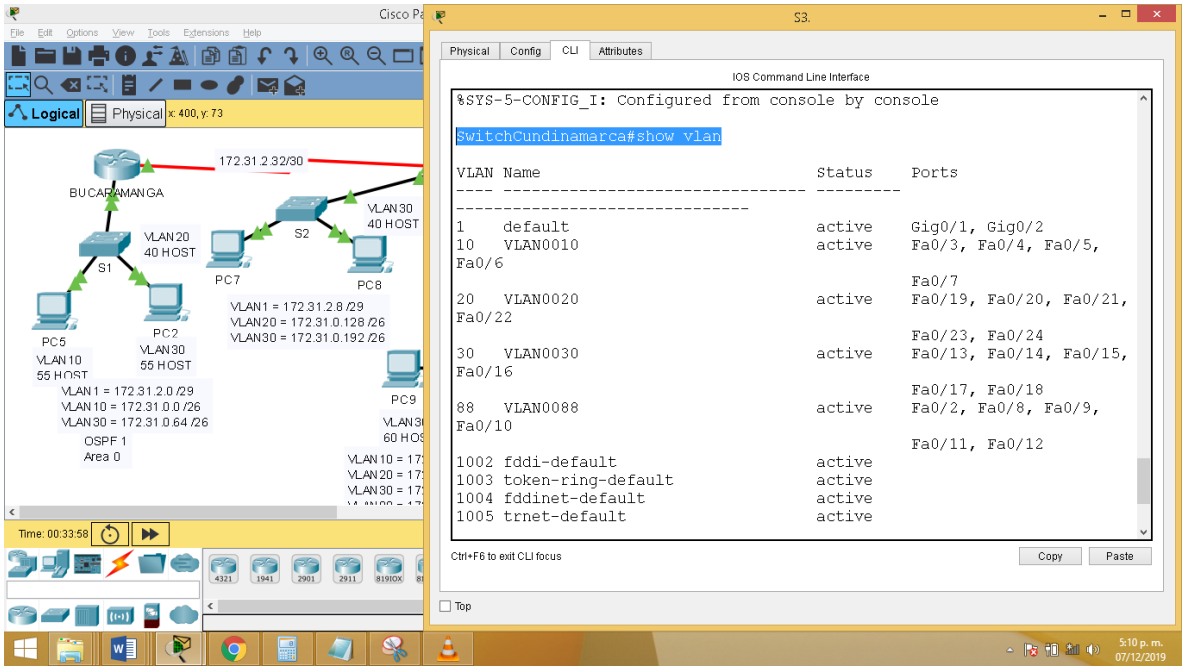
SwitchCundinamarca(config-vlan)#*vlan 88*

SwitchCundinamarca(config-vlan)#*exit*

SwitchCundinamarca(config)#*end*

Asignando puertos a vlans.

Figura 62. Asignación de puertos a VLANs



Fuente 71. prueba de habilidades prácticas, Autor: Javier Bulla

Autor: Javier Felipe Bulla

Para asignar puertos a VLANs, se ejecuta el siguiente comando.

SwitchCundinamarca(config)#*interface range f0/3 - 13*

SwitchCundinamarca(config-if-range)#*switchport access vlan 20*

SwitchCundinamarca(config-if-range)#*exit*

Se asignan los puertos o rangos según lo requerido.

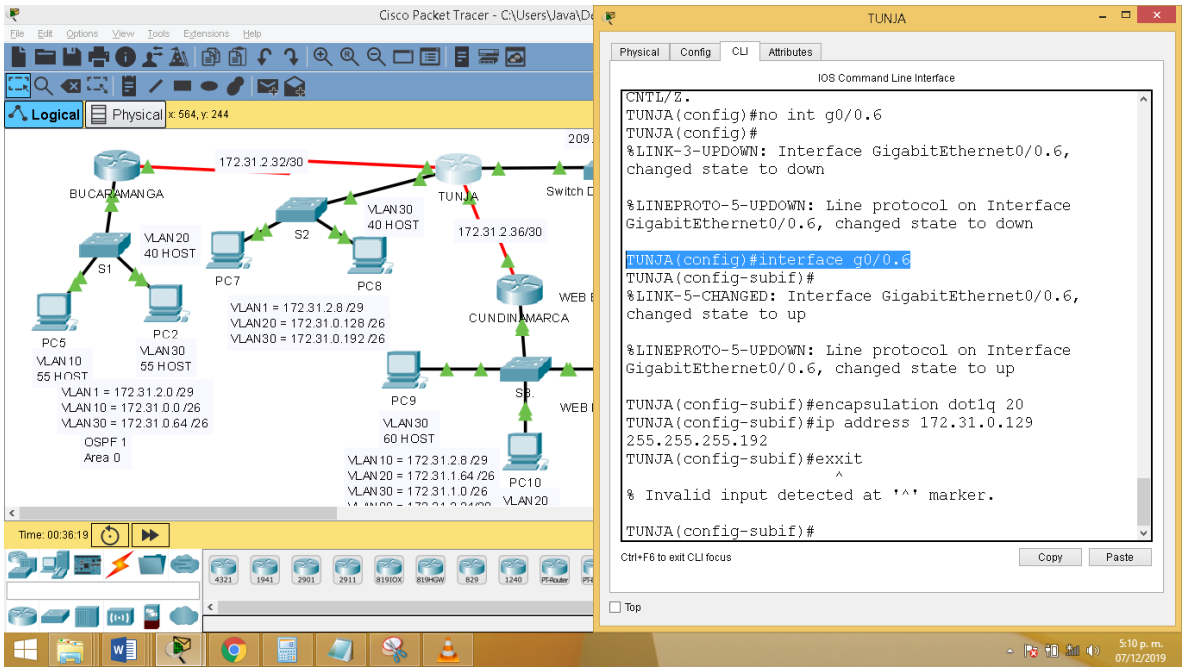
De igual modo para verificar el correcto funcionamiento se ejecuta el comando show vlan.

SwitchCundinamarca#*show vlan*

4.2.3. Parte 3. Enrutamiento De Vlans

4.2.3.1 Enrutamiento vlans de subred Tunja.

Figura 63. Enrutando vlans de subred Tunja.



Fuente 72. prueba de habilidades prácticas, Autor: Javier Bulla

Para el enrutamiento de la vlans de la subred Tunja, se ejecuta el siguiente código:

TUNJA(config)#interface g0/0.6

TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192

TUNJA(config-subif)#encapsulation dot1Q 20

TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192

TUNJA(config-subif)#exit

Permite en rutar por la interface g0/0.6, para la vlan 20

De igual modo se realiza el mismo proceso para la vlan 30.

TUNJA(config)#interface g0/0.24

TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192

TUNJA(config-subif)#encapsulation dot1Q 30

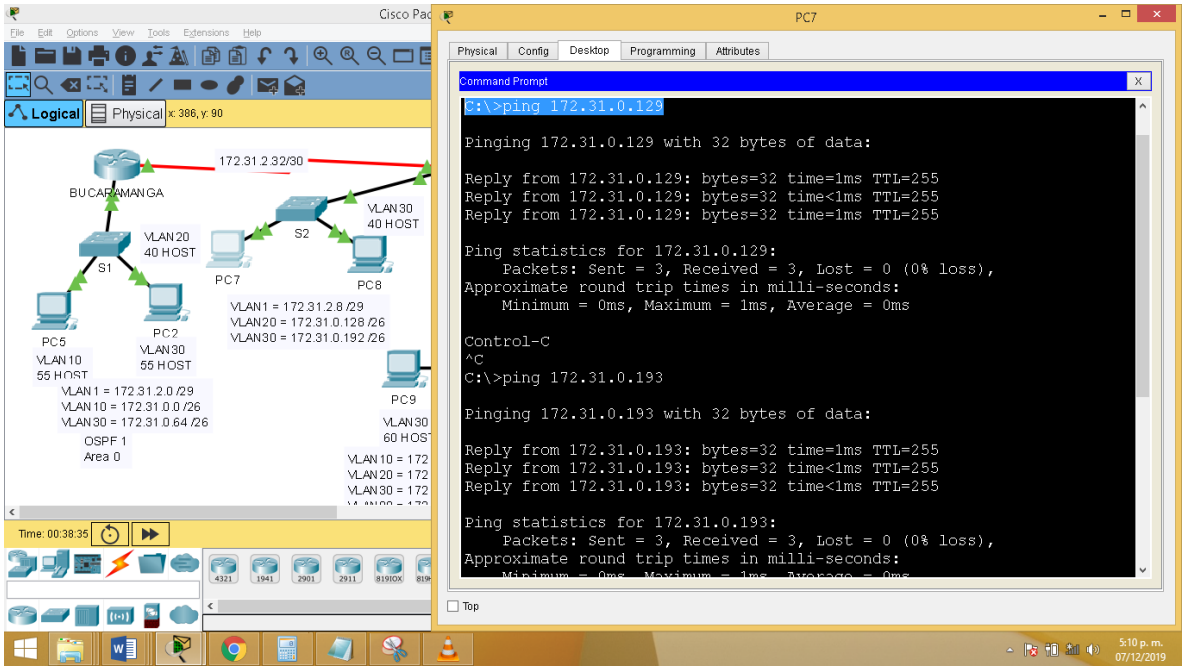
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192

TUNJA(config-subif)#exi

4.2.3.1.1 Verificando Conectividad.

Se realiza una prueba de conectividad para ello se realiza un ping.

Figura 64. verificando conectividad entre vlans



Fuente 73. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la conectividad entre vlans, se ejecuta los siguientes comandos:

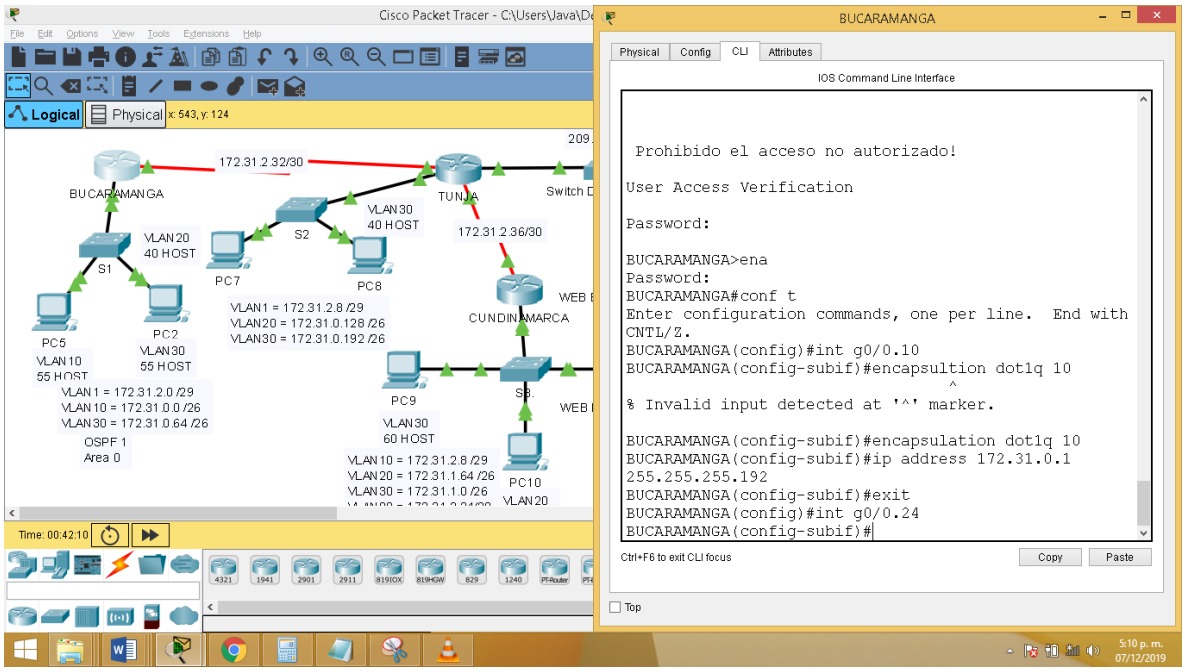
C:\>ping 172.31.0.129 → puerta de enlace de la vlan 20, resultado exitoso

C:\>ping 172.31.0.193 → puerta de entlace vlan 30, resultado exitoso.

C:\>ping 172.31.0.194 → dispositivo de vlan 30, PC 3, resultado exitoso.

4.2.3.2 Enrutamiento de vlans Router Bucaramanga.

Figura 65. Enrutamiento vlans router Bucaramanga



Fuente 74. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el enrutamiento en el router Bucaramanga, se ejecuta n los siguientes comandos:

BUCARAMANGA(config)#interface g0/0.10

BUCARAMANGA(config-subif)#encapsulation do

BUCARAMANGA(config-subif)#encapsulation dot1Q 10

BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192

BUCARAMANGA(config-subif)#exit

BUCARAMANGA(config)#interface g0/0.24

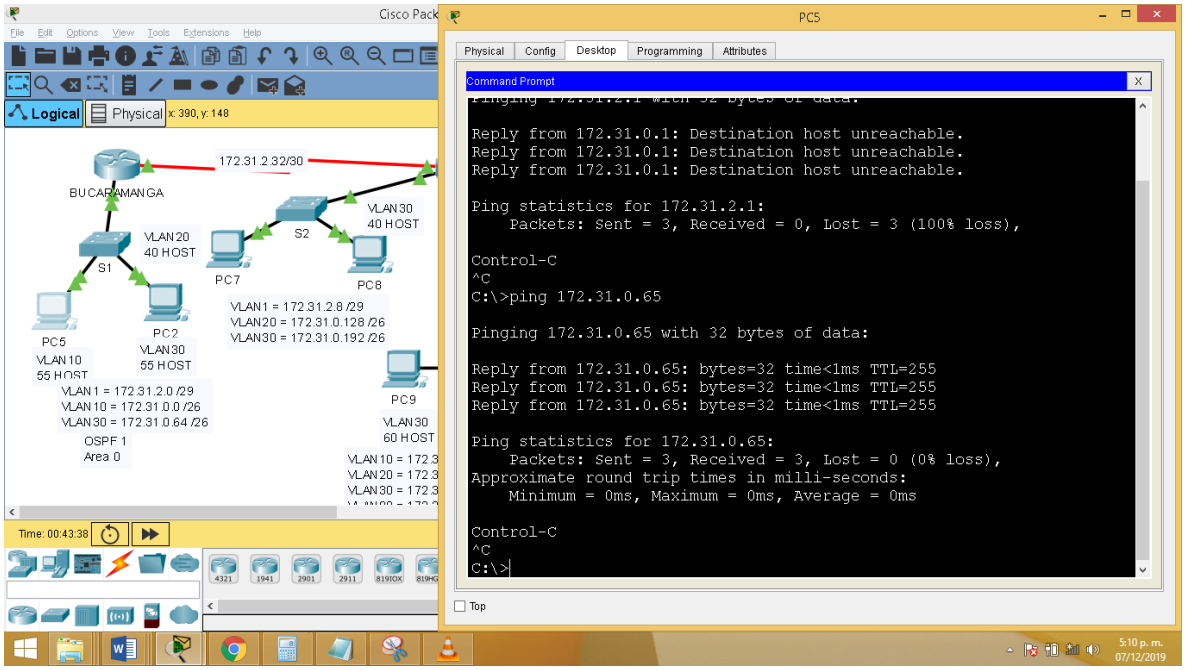
BUCARAMANGA(config-subif)#encapsulation dot1Q 30

BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192

BUCARAMANGA(config-subif)#exit

4.2.3.2.1 Verificando Conectividad.

Figura 66. verificando conectividad de enrutamiento, router Bucaramanga



Fuente 75. prueba de habilidades prácticas, Autor: Javier Bulla

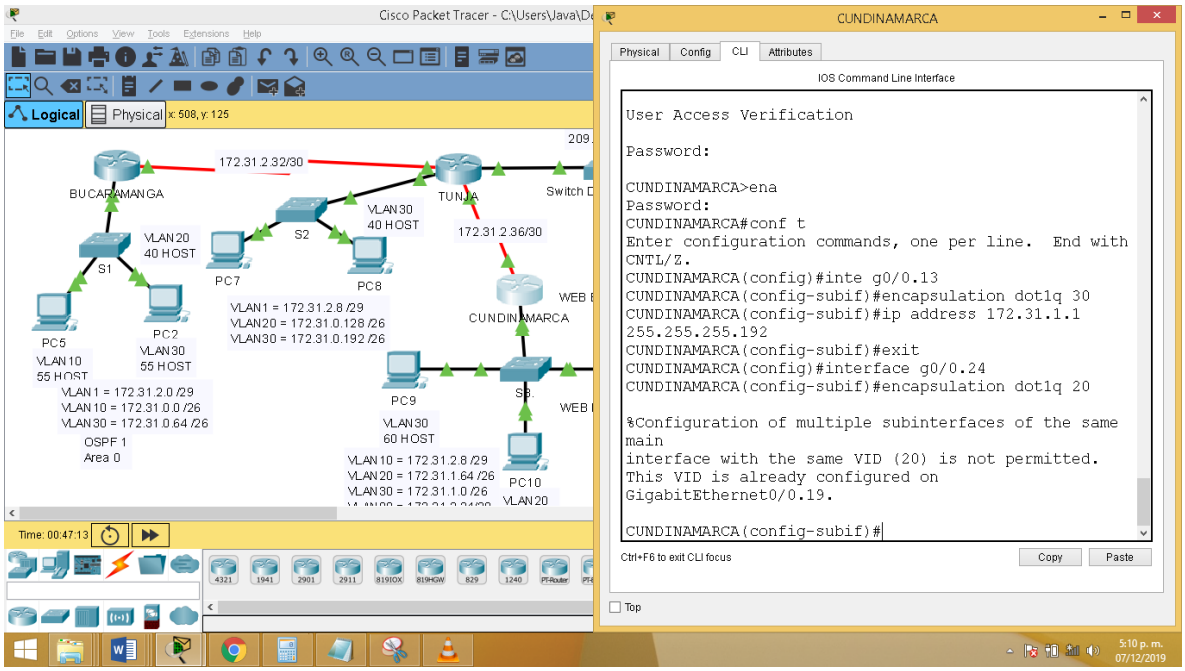
Para verificar que la configuración es exitosa, se procede a ejecutar el comando ping.

C:\>ping 172.31.2.1 → dirección de enlace de la vlan 10, resultado exitoso.

C:\>ping 172.31.0.65 → dirección de enlace de la vlan 30, resultado exitoso.

4.2.3.4. Enrutamiento de vlans Router Cundinamarca.

Figura 67. Enrutamiento vlans router, Cundinamarca



Fuente 76. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el enrutamiento de las vlans en el router Cundinamarca, para tal efecto, se ejecuta los siguientes datos:

CUNDINAMARCA(config)#interface g0/0.13

CUNDINAMARCA(config-subif)#encapsulation dot1Q 30

CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192

CUNDINAMARCA(config-subif)#exit

CUNDINAMARCA(config)#interface g0/0.24

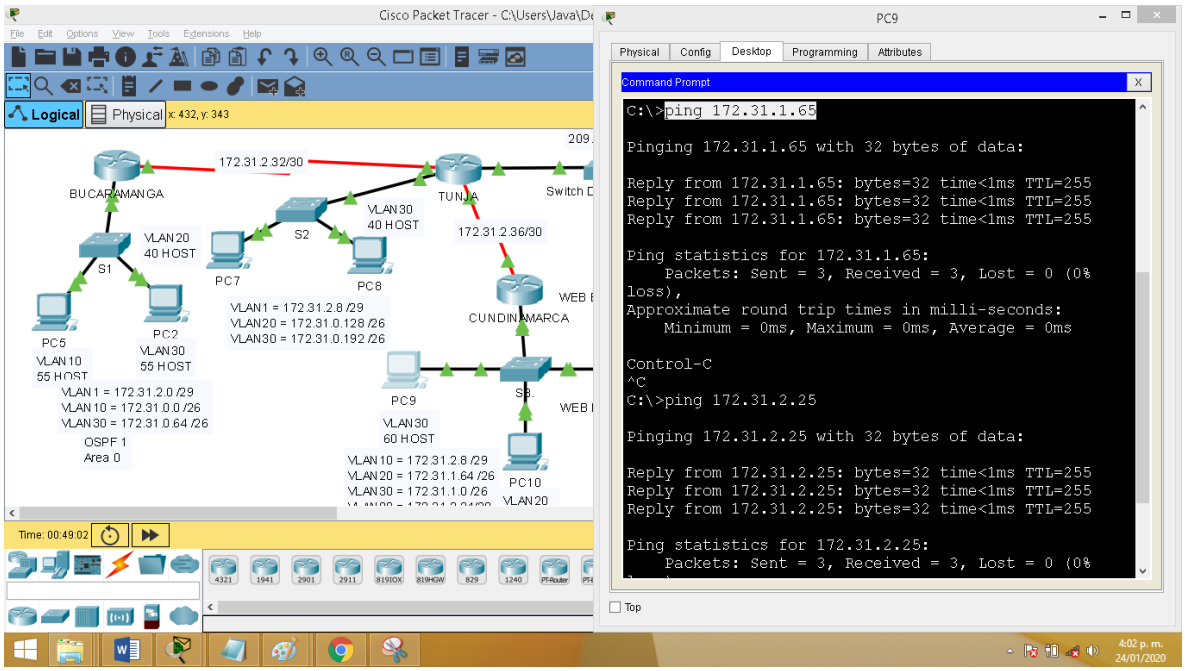
CUNDINAMARCA(config-subif)#encapsulation dot1Q 20

CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192

CUNDINAMARCA(config-subif)#exit

4.2.3.4.1 Verificando enrutamiento de vlans en router Cundinamarca.

Figura 68. Verificando conectividad de enrutamiento, router Cundinamarca



Fuente 77. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la conectividad de enrutamiento de las vlans, se ejecuta el comando PING.

Comandos:

C:\>ping 172.31.1.1 → enlace vlan 30, Resultado exitoso.

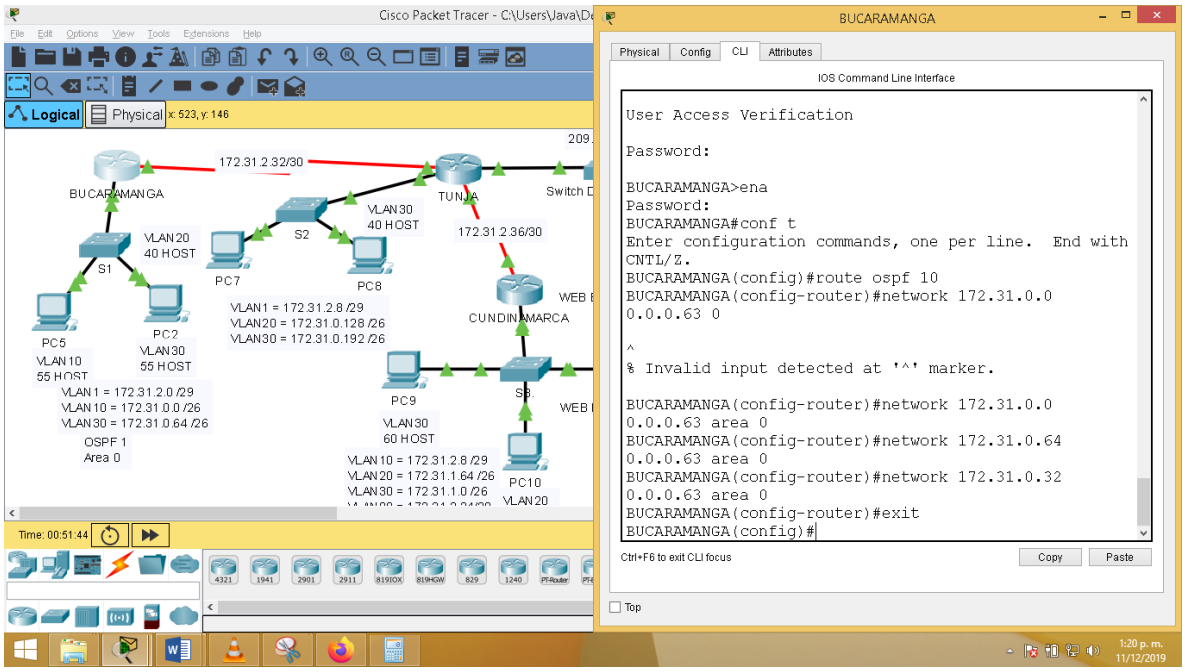
C:\>ping 172.31.1.65 → enlace vlan 20, Resultado exitoso.

C:\>ping 172.31.2.25 → enlace vlan 88, Resultado exitoso.

4.2.4. Parte 4. Protocolo De Enrutamiento Ospf

4.2.4.1. Protocolo de enrutamiento OSPF en router Bucaramanga.

Figura 69. OSPF en router Bucaramanga



Fuente 78. prueba de habilidades prácticas, Autor: Javier Bulla

Para implementar el protocolo OSPF, se ejecuta los siguientes comandos:

BUCARAMANGA(config)#route ospf 18

BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0

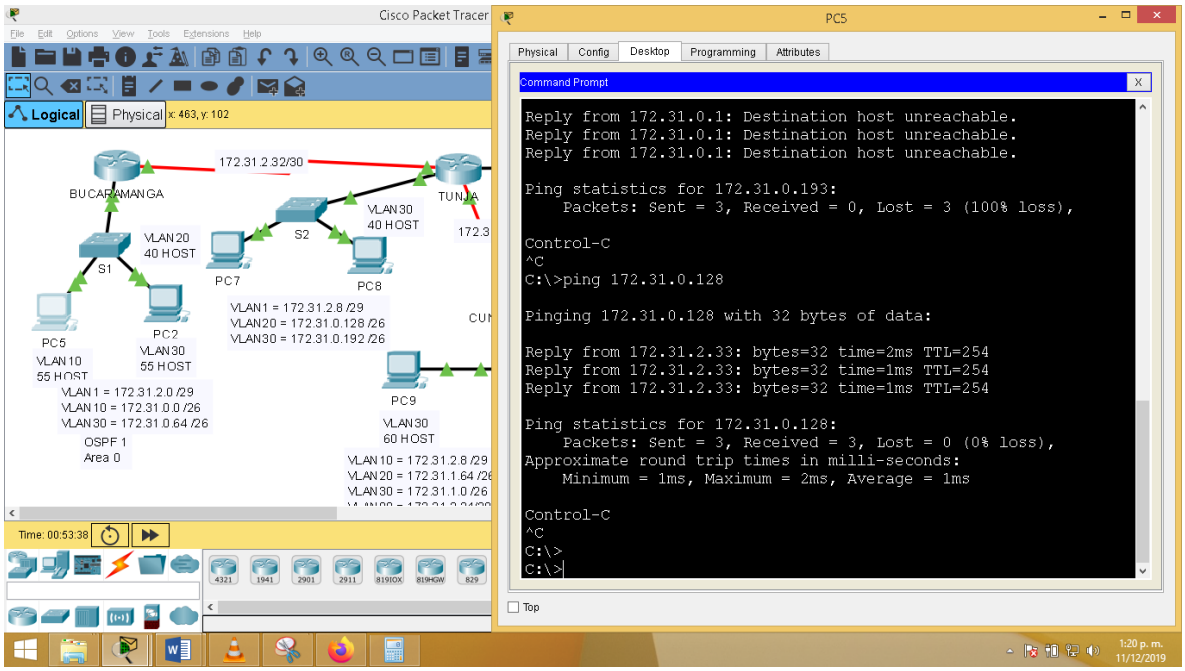
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0

BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0

BUCARAMANGA(config-router)#exit

4.2.4.1.1 Verificando conectividad con Redes y SubRedes Externas.

Figura 70. Verificando conectividad en redes externas



Fuente 79. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la conectividad, se ejecutan los siguientes comandos:

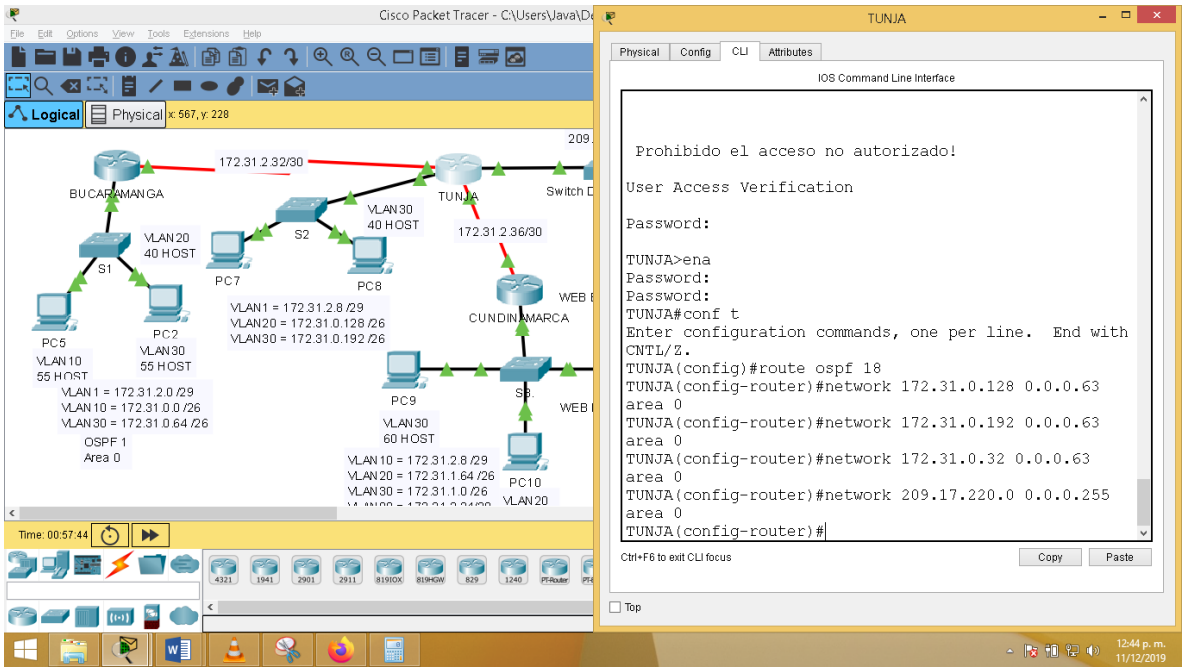
C:\>ping 209.17.220.2 → Servidor externo WEB, resutlado Exitoso.

C:\>ping 172.31.0.193 → enlace, vlan 30, de subred Tunja, resultado Exitoso.

C:\>ping 172.31.0.128 → enlace, vlan 20, de subred Tunja, resultado Exitoso.

4.2.4.2. Protocolo de enrutamiento OSPF en router Tunja

Figura 71. OSPF en router Tunja



Fuente 80. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el router tunja, bajo el protocolo OSPF, se ejecutan los siguientes comandos:

TUNJA#configure terminal

TUNJA(config)#route ospf 18

TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0

TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0

TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0

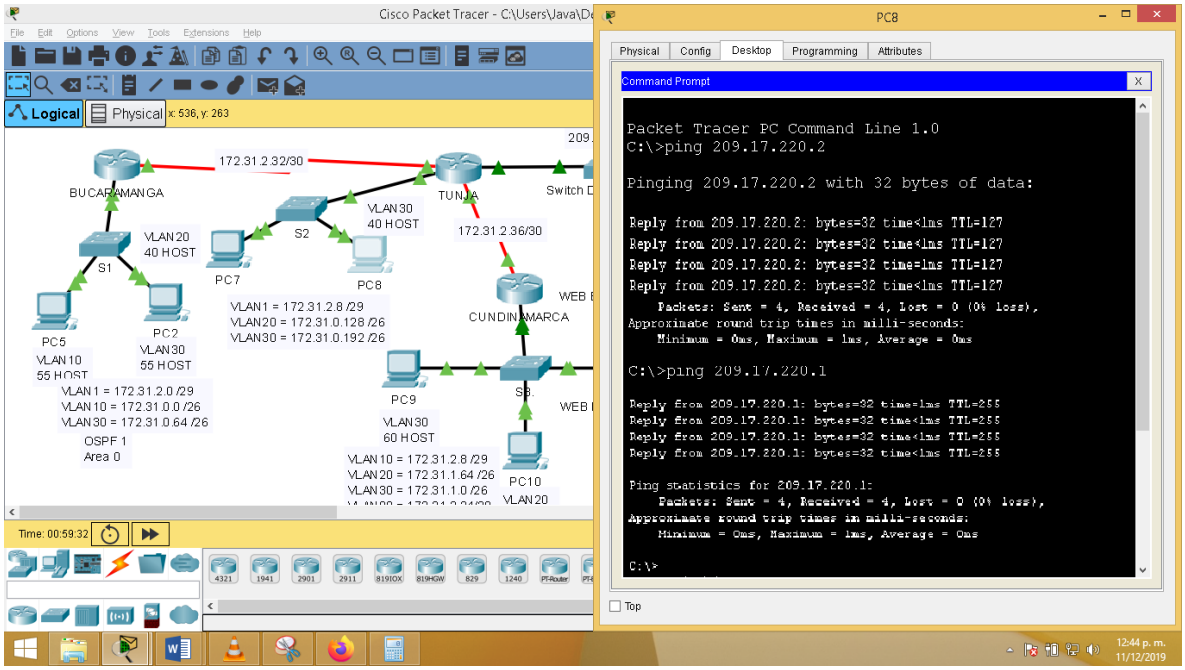
TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0

TUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0

De tal manera que se implemente el protocolo OSPF y se tenga conexión con otras redes.

4.2.4.2.1 Verificando conectividad con Redes y SubRedes Externas.

Figura 72. Verificando conexión



Fuente 81. prueba de habilidades prácticas, Autor: Javier Bulla

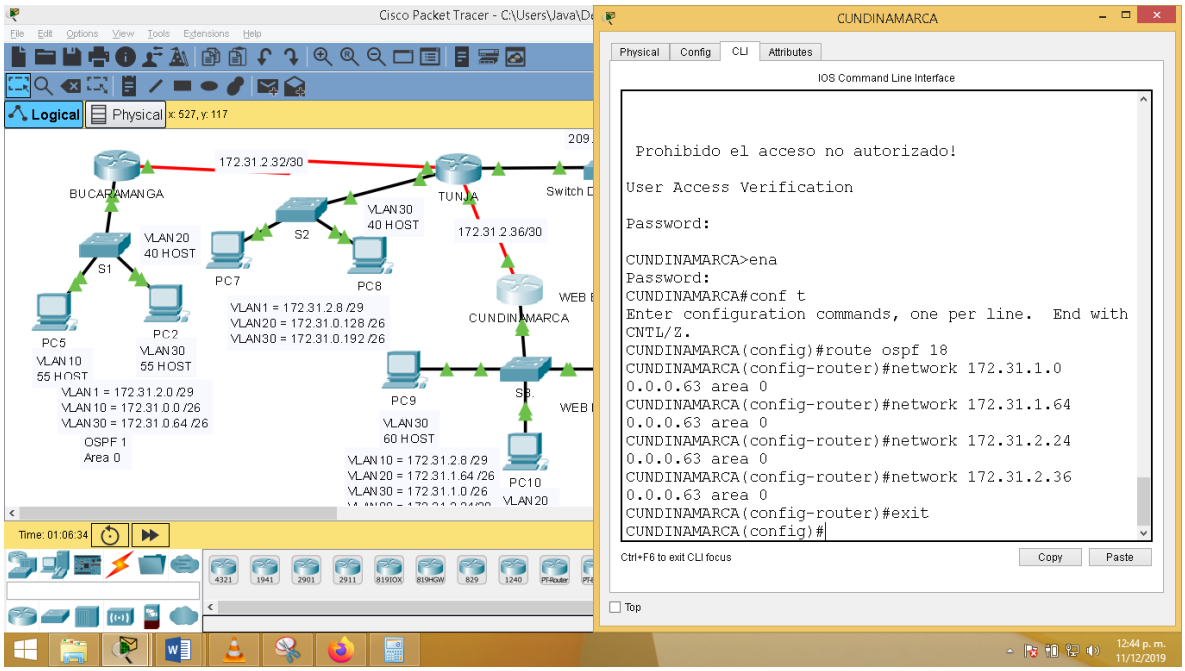
Para verificar la correcta implementación del protocolo OSPF, se ejecuta el comando PING, para tal efecto se realizará con las direcciones públicas.

C:\>ping 209.17.220.2 → Dirección IP, del servidor WEB externo, Resultado exitoso

C:\>ping 209.17.220.1 → Dirección IP, salida de router Tunja, Resultado exitoso.

4.2.4.3 Protocolo de enrutamiento OSPF en router Cundinamarca.

Figura 73. OSPF router Cundinamarca



Fuente 82. prueba de habilidades prácticas, Autor: Javier Bulla

Para implementar el protocolo de enrutamiento OSPF, en el router Cundinamarca, se ejecutan lo siguientes comandos:

CUNDINAMARCA#configure terminal

CUNDINAMARCA(config)#route ospf 18

CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0

CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0

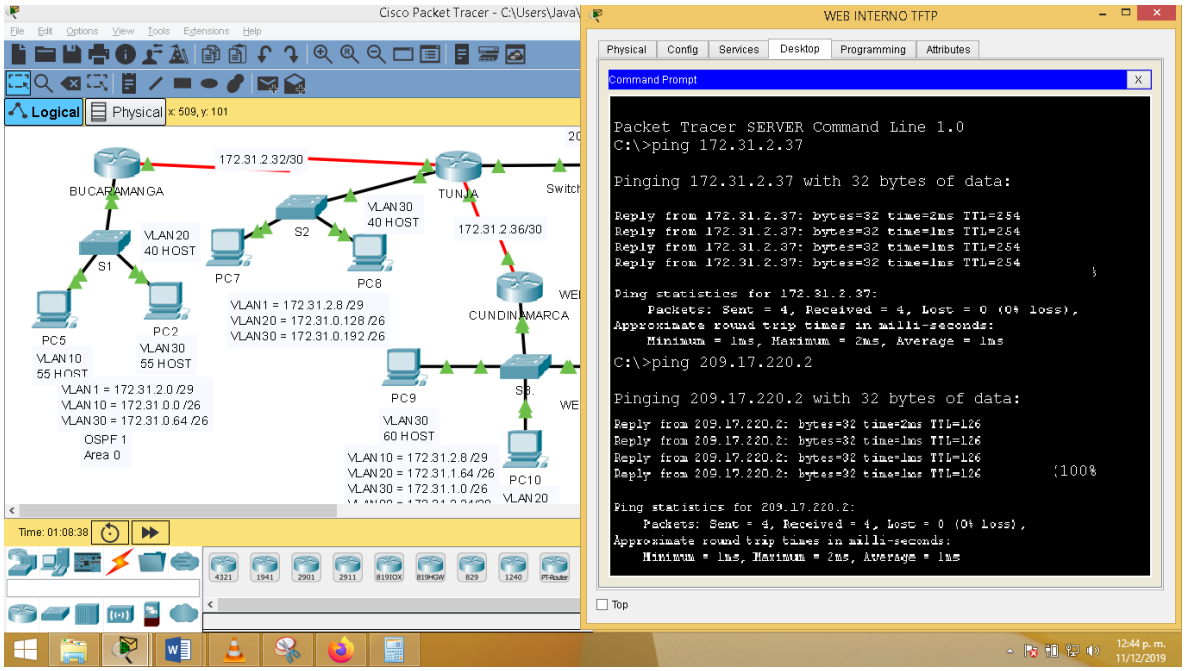
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0

CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0

CUNDINAMARCA(config-router)#exit

4.2.4.3.1 Verificando conectividad con Redes y SubRedes Externas.

Figura 74. Verificando conectividad de red.



Fuente 83. prueba de habilidades prácticas, Autor: Javier Bulla.

Para verificar que hay comunicación, la red 172.31.0.0/19, se ejecuta el comando PING.

C:\>ping 172.31.2.37 → enlace de entrada router Tunja, resultado exitoso.

C:\>ping 209.17.220.2 → Servidor WEB Externo, Resultado Exitoso.

C:\>ping 172.31.2.34 → Enlace de entrad router Bucaramanga, resultado exitoso.

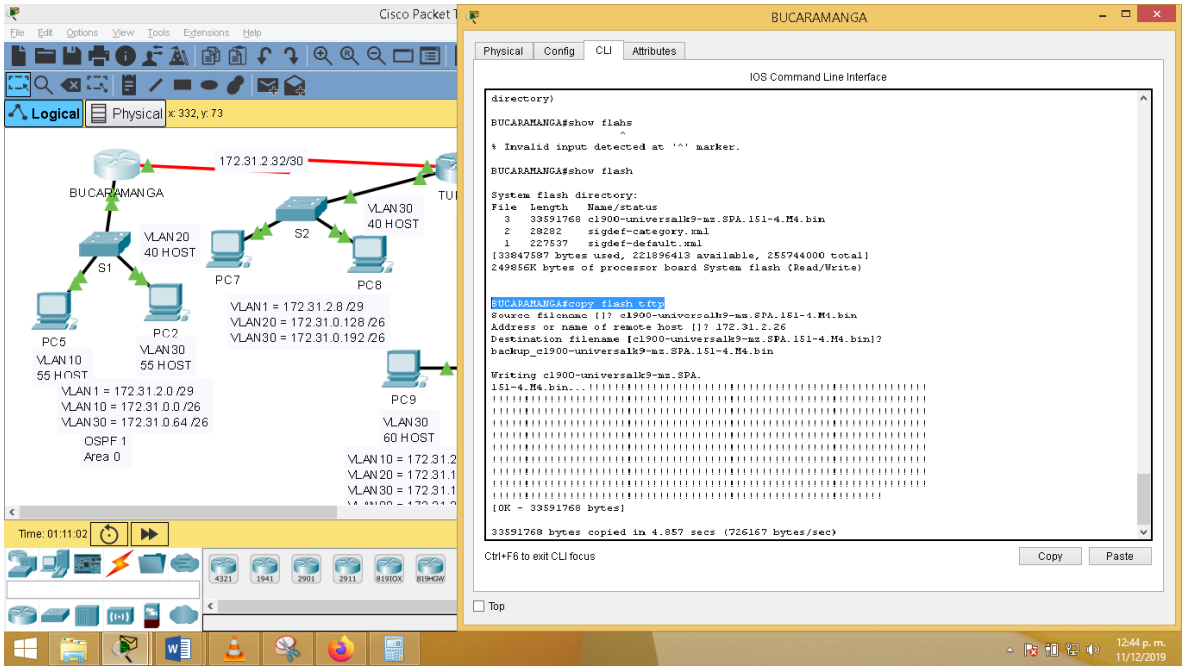
C:\>ping 172.31.0.2 → dirección IP, PC5, subred Bucaramanga, Resultado exitoso.

C:\>ping 172.31.0.129 → dirección IP, PC7, subred Tunja, Resultado exitoso.

4.2.4.4 Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers

BUCARAMANGA

Figura 75. prueba de habilidades prácticas, Autor: Javier Bulla.



Fuente 84. prueba de habilidades prácticas, Autor: Javier Bulla.

Para realizar backups, archivos de configuración de TFTP,

BUCARAMANGA>enable

BUCARAMANGA#copy running-config tftp

BUCARAMANGA#copy flash tftp →

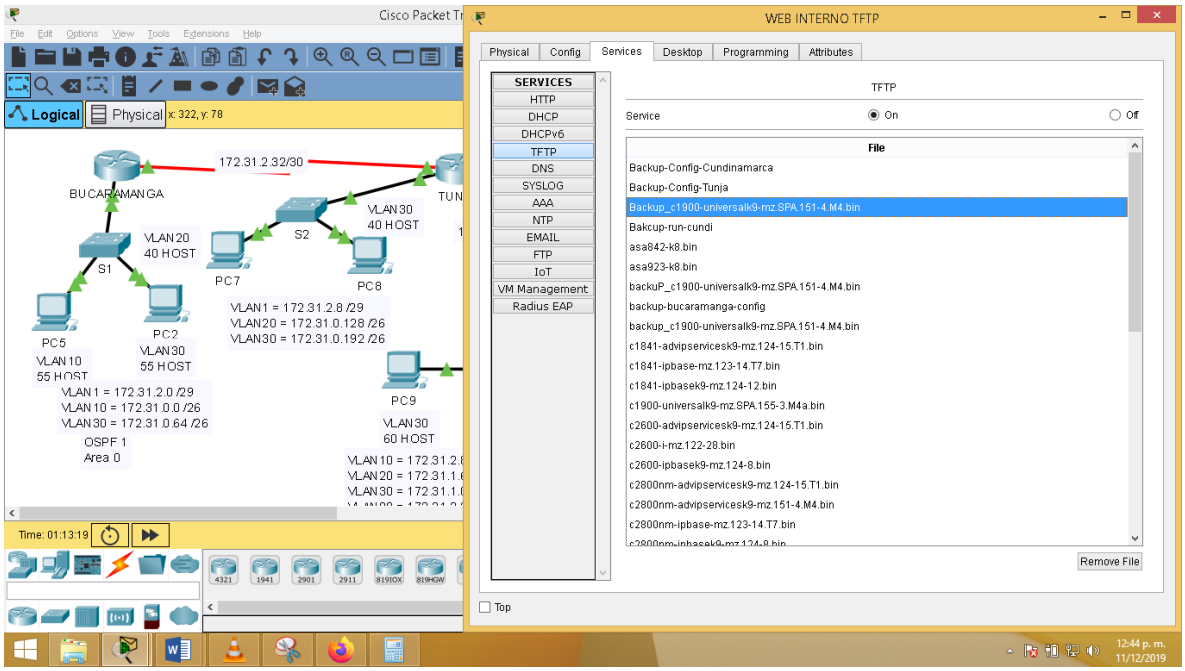
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin

Address or name of remote host []? 172.31.2.26

Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? backup_c1900-universalk9-mz.SPA.151-4.M4.bin

De tal manera que se crea una copia de la imagen de configuración del router.

Figura 76. Verificando Backups en servidor TFTP

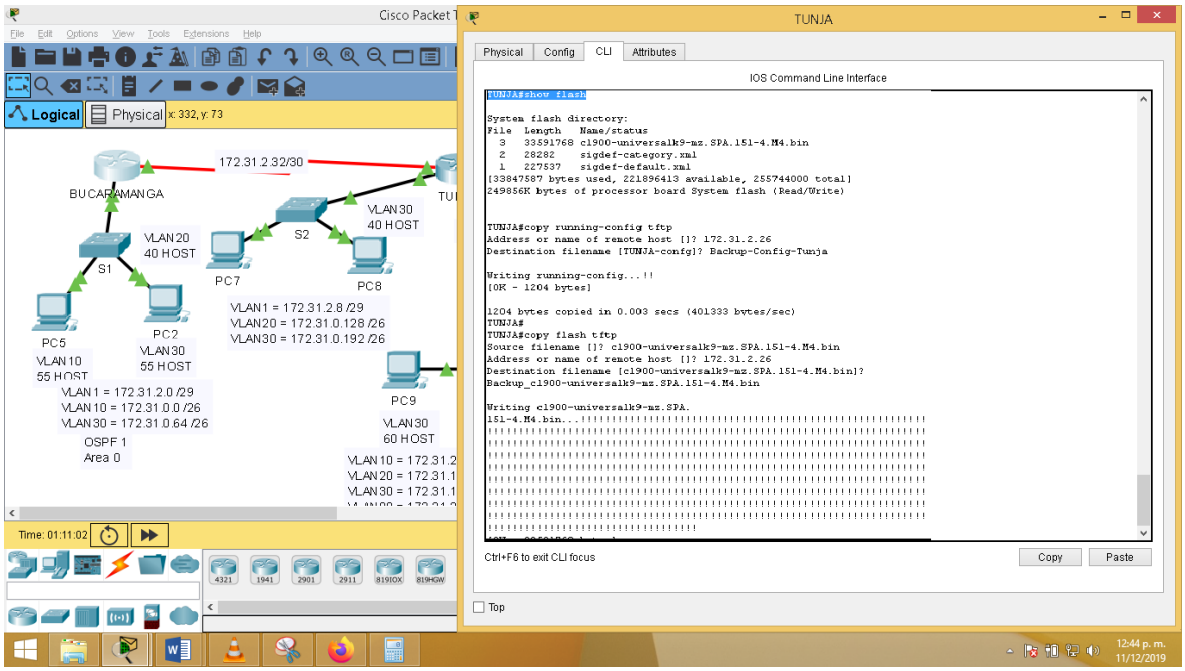


Fuente 85. prueba de habilidades prácticas, Autor: Javier Bulla

Se puede verificar que se realizó con éxito las copias de los archivos del router.

Tunja

Figura 77. Backups a TFTP configuración router Tunja



Fuente 86. prueba de habilidades prácticas, Autor: Javier Bulla

Para realizar backups, archivos de configuración de TFTP.

TUNJA#copy running-config tftp

Address or name of remote host []? 172.31.2.26

Destination filename [TUNJA-confg]? Backup-Config-Tunja

TUNJA#copy flash tftp

Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin

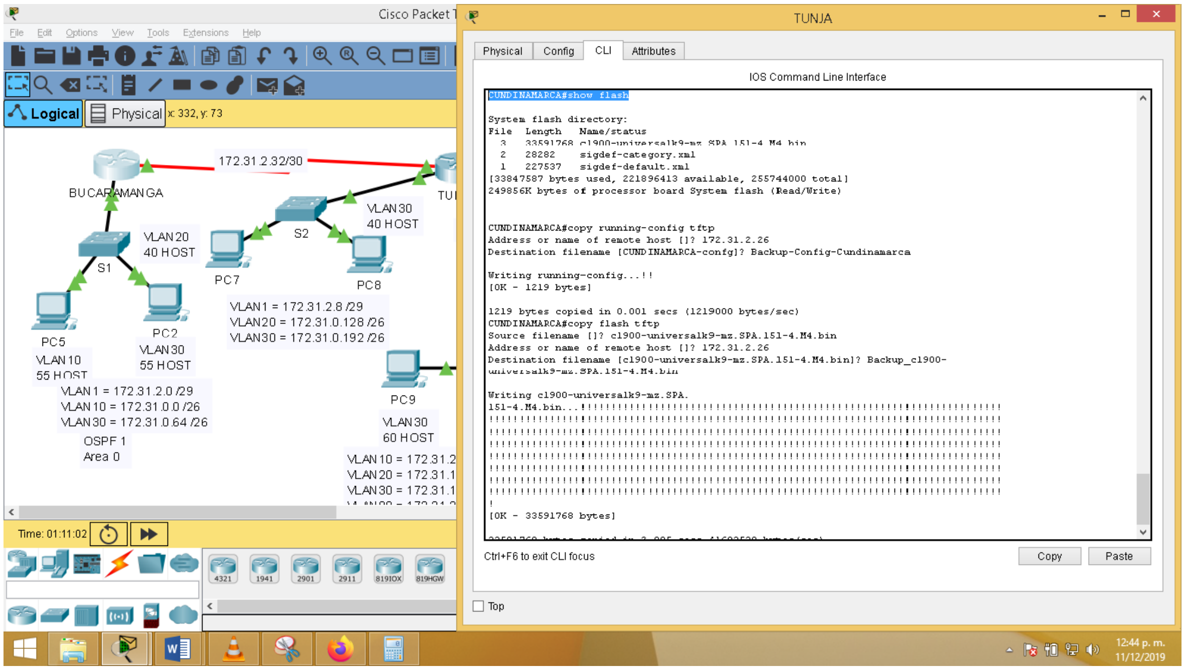
Address or name of remote host []? 172.31.2.26

Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? Backup_c1900-universalk9-mz.SPA.151-4.M4.bin

Se puede verificar que la configuración, se realizó exitosamente y que se cumplió a cabalidad las copias de la configuración del router Tunja.

Cundinamarca.

Figura 78. Backups a TFTP configuración router Cundinamarca



Fuente 87. prueba de habilidades prácticas, Autor: Javier Bulla

Para realizar backups, archivos de configuración de TFTP

CUNDINAMARCA#copy running-config tftp

Address or name of remote host []? 172.31.2.26

Destination filename [CUNDINAMARCA-confg]? Backup-Config-Cundinamarca

Configuración router Tunja .

CUNDINAMARCA#copy flash tftp

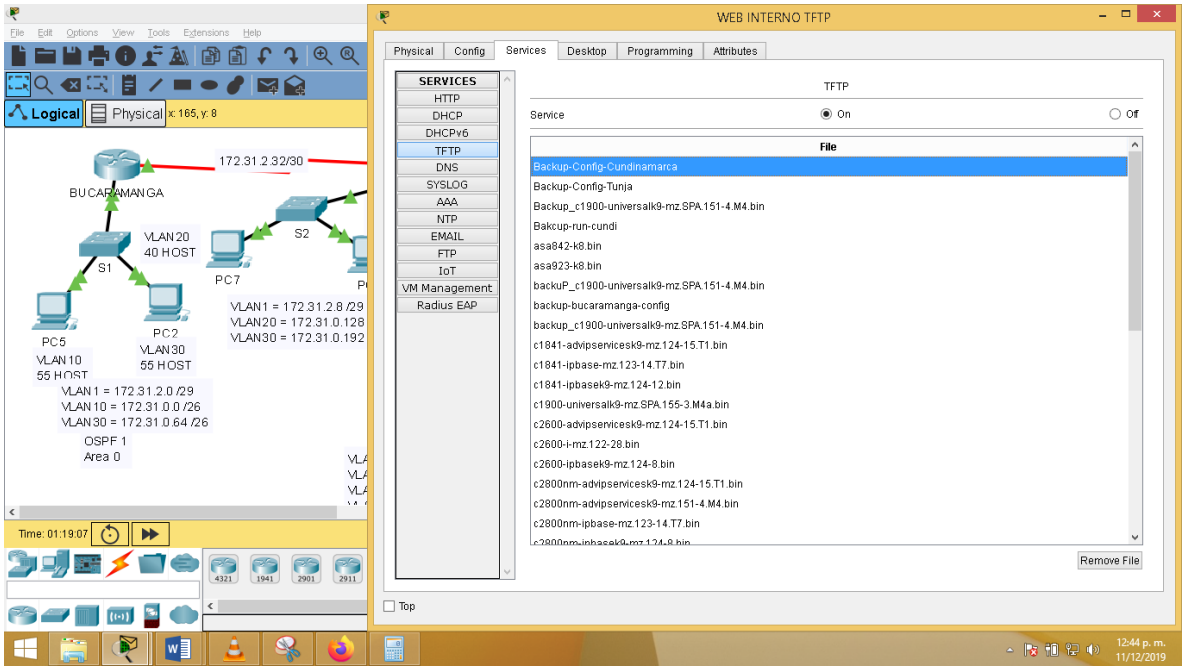
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin

Address or name of remote host []? 172.31.2.26

Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? Backup_c1900-universalk9-mz.SPA.151-4.M4.bin

4.2.4..4.1 Verificacion De Backups

Figura 79. Verificación de implementación de Bakcups



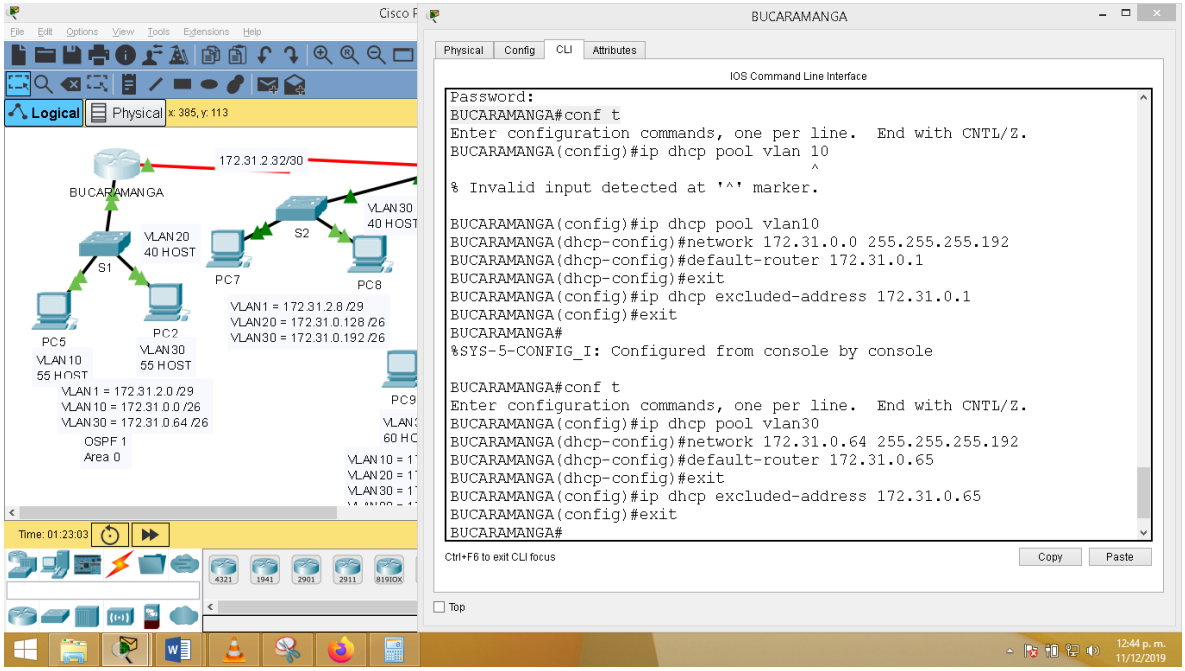
Fuente 88. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar si fueron generados con éxito los backups, de cada router, se accede al servidor TFTP, como se puede visualizar los archivos de configuración de inicio y las imágenes de SO, están en el servidor TFTP.

4.2.5. Parte 5. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca.

Configurando router Bucaramanga para asignar direcciones por protocolo DHCP.

Figura 80. Configurando Pool de subred en router Bucaramanga



Fuente 89. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el router Bucaramanga se ejecutan los siguientes comandos, los cuales permitirán que el router asigne un comportamiento de servidor DHCP y asigne direcciones IP, de forma dinámica a cualquier dispositivo que esté conectado en la sub red, según la vlan.

Comandos, para la vlan 10

Router(config)*#ip dhcp pool VLAN10*

Router(dhcp-config)*#network 172.31.0.0 255.255.255.192*

Router(dhcp-config)*#default-router 172.31.0.1*

Router(dhcp-config)*#exit*

Router(config)#*ip dhcp excluded-address 172.31.0.1*

Router(config)#*exit*

Comandos, para la vlan 30.

Router(config)#*ip dhcp pool VLAN30*

Router(dhcp-config)#*network 172.31.0.64 255.255.255.192*

Router(dhcp-config)#*default-router 172.31.0.65*

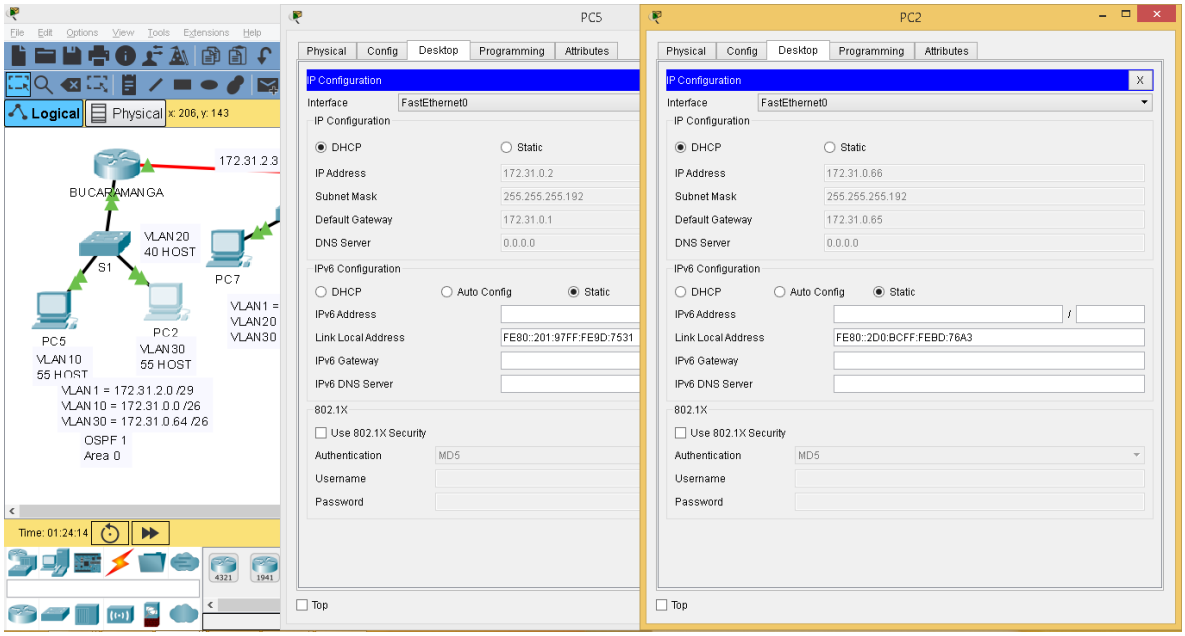
Router(dhcp-config)#*exit*

Router(config)#*ip dhcp excluded-address 172.31.0.65*

Router(config)#*exit*

Comprobación de direcciones asignadas de forma dinámica por protocolo DHCP.

Figura 81. Asignación de direcciones IP a PCs en la subred Bucaramanga

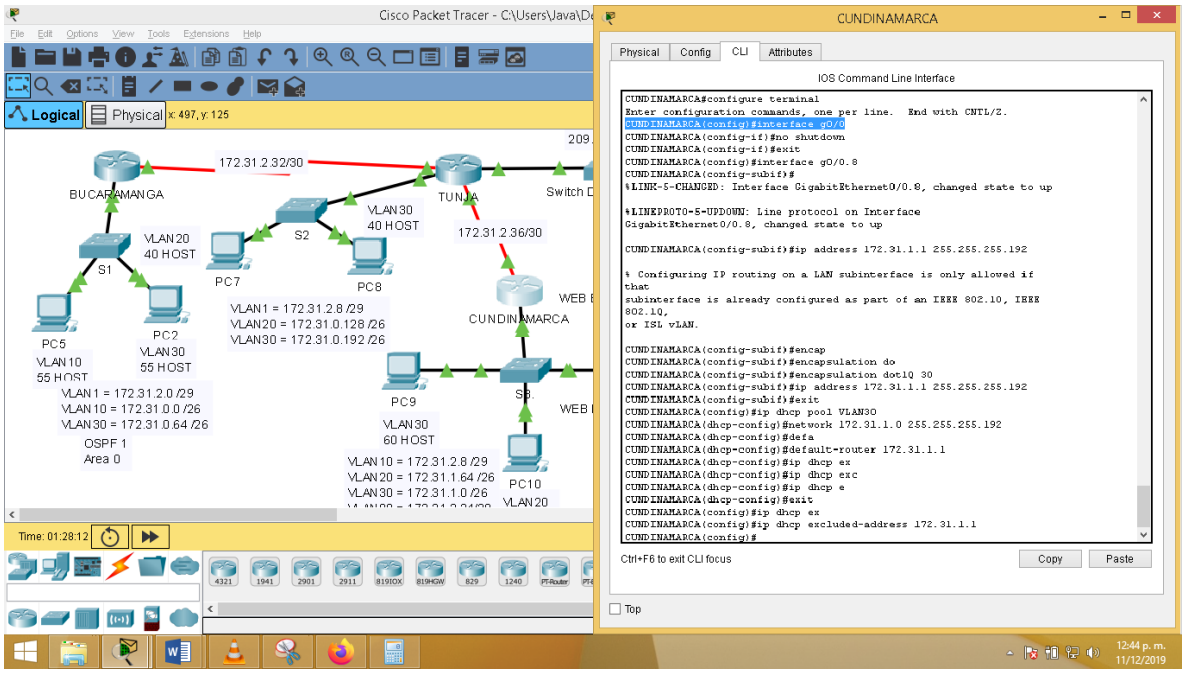


Fuente 90. prueba de habilidades prácticas, Autor: Javier Bulla

Se puede verificar que cualquier puerto que está en cada rango de la vlan se le asigna una dirección IP de forma dinámica, cabe aclarar que cada vlan tiene su propia subred.

Configuración DHCP, en el router Cundinamarca

Figura 82. Configurando puerto para asignación DHCP por parte del router Cundinamarca



Fuente 91. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el router Cundinamarca, en el cual se permita asignar direcciones IP de forma dinámica a los hosts que están conectados a una vlan previamente creada, se ejecutan los siguientes comandos.

CUNDINAMARCA(config)#*ip dhcp pool VLAN30*

CUNDINAMARCA(dhcp-config)#*network 172.31.1.0 255.255.255.192*

CUNDINAMARCA(dhcp-config)#*default-router 172.31.1.1*

CUNDINAMARCA(dhcp-config)#*exit*

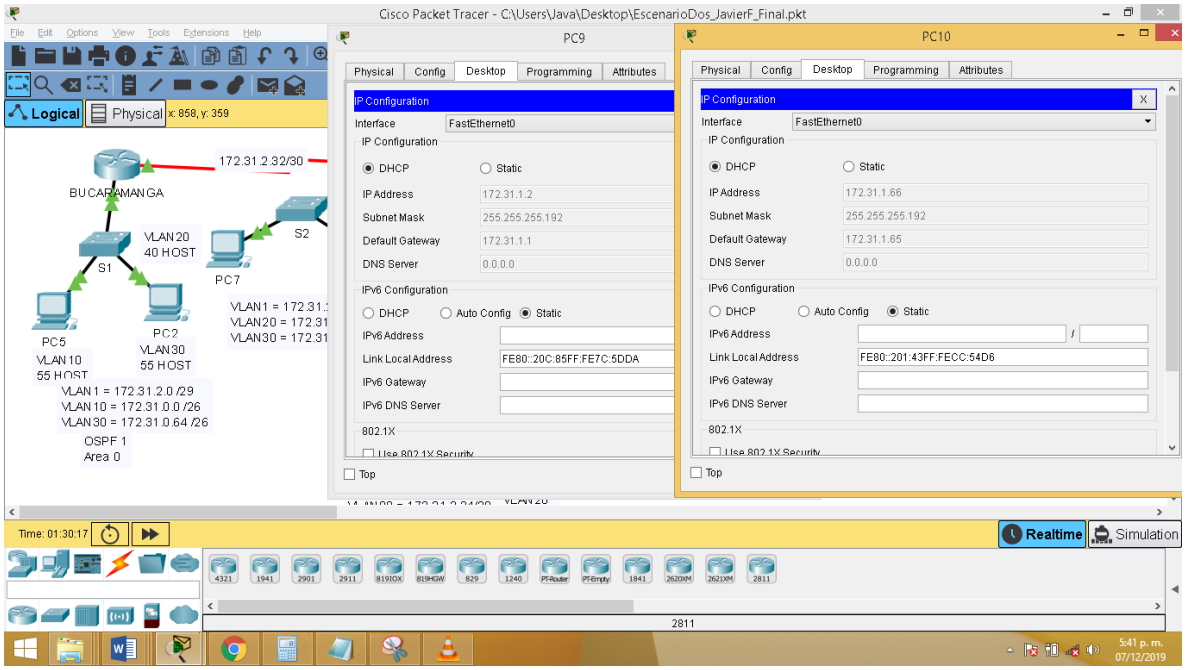
CUNDINAMARCA(config)#*ip dhcp excluded-address 172.31.1.1*

CUNDINAMARCA(config)#*exit*

De igual modo se repite el proceso con las respectivas interfaces a las que fueron asignadas en la vlan.

Comprobación de implementación.

Figura 83. Verificación asignación de dirección IP de forma dinámica



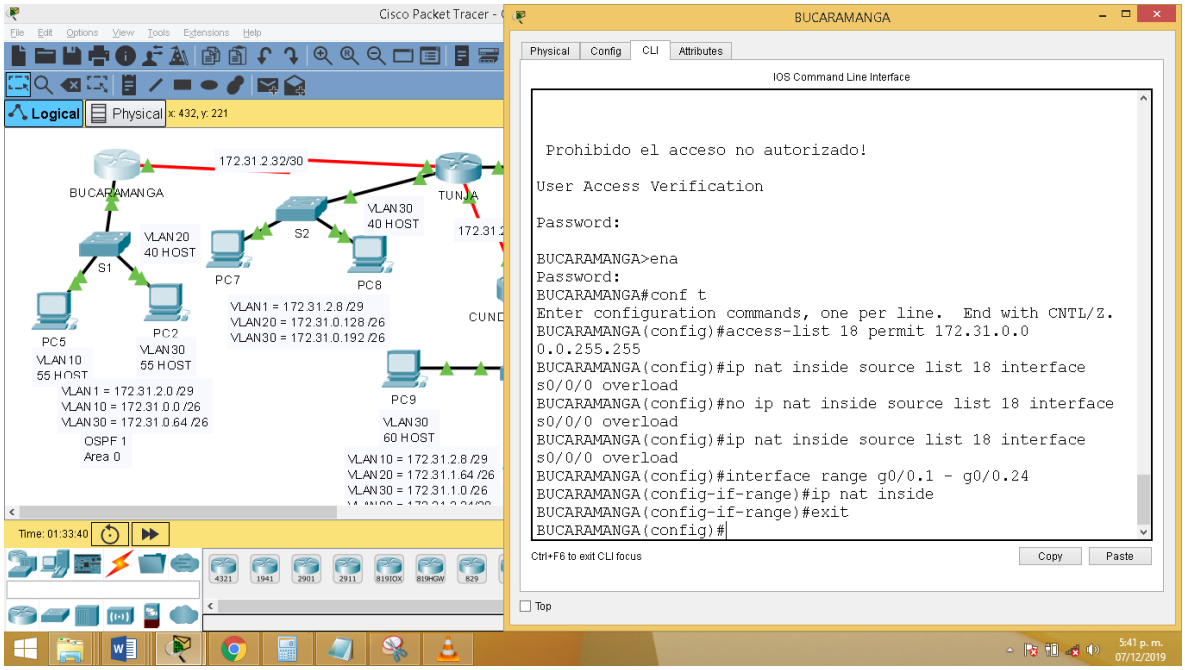
Fuente 92. prueba de habilidades prácticas, Autor: Javier Bulla

Se puede comprobar que las direcciones IP son asignadas de forma correcta por parte del router a los dispositivos, se puede verificar que cada vlan tiene una subred diferente, por tal motivo la asignación IP, debe estar de acuerdo a cada subdominio de la red.

4.2.6. Parte 6. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

Configuración NAT router Bucaramanga.

Figura 84. NAT (PAT) router Bucaramanga



Fuente 93. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar NAT (PAT) en el router Bucaramanga se ejecuta los siguientes comandos:

BUCARAMANGA(config)#access-list 18 permit 172.31.0.0 0.0.255.255

BUCARAMANGA(config)#ip nat inside source list 18 interface s0/0/0 overload

BUCARAMANGA(config)#no ip nat inside source list 18 interface s0/0/0 overload

BUCARAMANGA(config)#ip nat inside source list 18 interface s0/0/0 overload

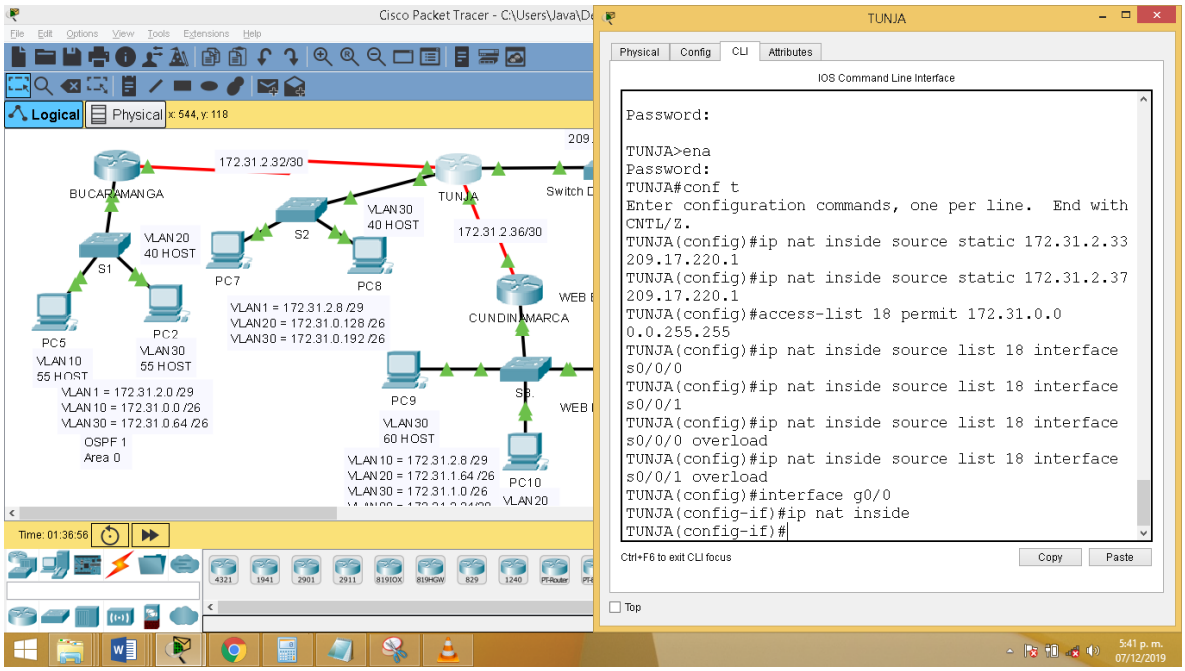
BUCARAMANGA(config)#interface range g0/0.1 - g0/0.24

BUCARAMANGA(config-if-range)#ip nat inside

BUCARAMANGA(config-if-range)#exit

Configuración NAT router Tunja

Figura 85. Protocolo NAT router Tunja



Fuente 94. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el router de Tunja con NAT, se ejecutan los siguientes comandos:

NAT estático:

COMANDOS:

TUNJA>enable

TUNJA#configure terminal

TUNJA(config)#ip nat inside sorce static 172.31.2.33 209.17.220.1

TUNJA(config)#ip nat inside source static 172.31.2.33 209.17.220.1

TUNJA(config)#ip nat inside source static 172.31.2.37 209.17.220.1

NAT dinamico (PAT)

COMANDOS

TUNJA(config)#access-list 18 permit 172.31.0.0 0.0.31.255

TUNJA(config)#ip nat inside source list 18 interface s0/0/0 overload

TUNJA(config)#ip nat inside source list 18 interface s0/0/1 overload

NAT INTERNOS

TUNJA(config-if)#interface s 0/0/0

TUNJA(config-if)#ip nat inside

TUNJA(config-if)#exit

TUNJA(config)#interface s 0/0/1

TUNJA(config-if)#ip nat inside

TUNJA(config-if)#exit

NATA EXTERNOS

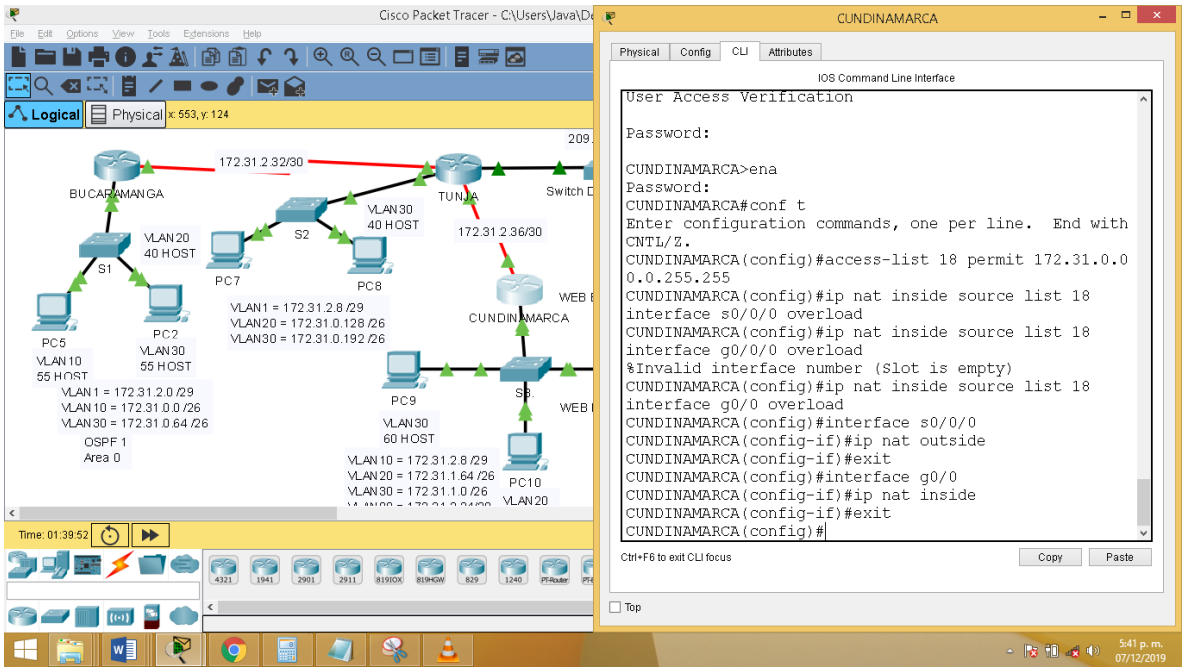
TUNJA(config)#interface g0/1

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#exit

Configuración NAT router Cundinamarca

Figura 86. Configuración NAT(PAT) router Cundinamarca



Fuente 95. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar NAT (PAT) en el router Cundinamarca, se ejecutan lo siguientes comandos:

CUNDINAMARCA(config)#ip nat inside source list 18 interface g0/0 overload

CUNDINAMARCA(config)#interface s0/0/0

CUNDINAMARCA(config-if)#ip nat outside

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#interface g0/0

CUNDINAMARCA(config-if)#ip nat inside

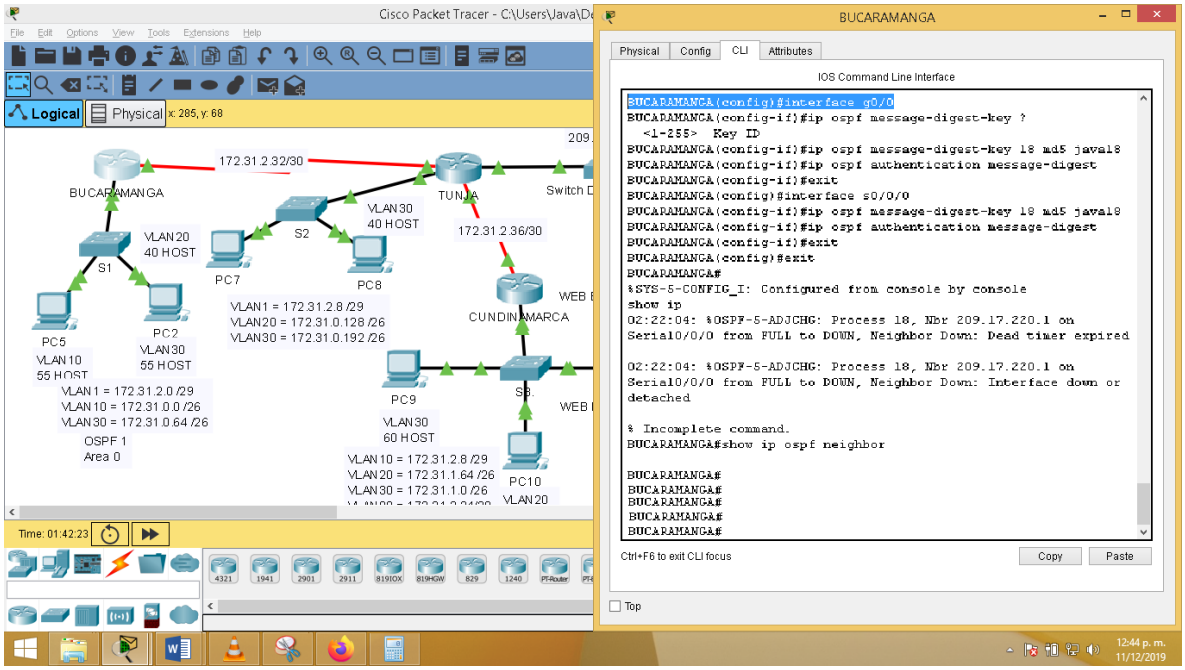
CUNDINAMARCA(config-if)#exit

4.2.7. Parte 7. El enrutamiento deberá tener autenticación.

4.2.7.1 AUTENTICACION OSPF

Autenticación OSPF MD5, router Bucaramanga.

Figura 87. Autenticación OSPF md5 router Bucaramanga.



Fuente 96. prueba de habilidades prácticas, Autor: Javier Bulla.

Para crear autenticación en la subred, se ejecuta los siguientes comandos:

BUCARAMANGA(config)#interface g0/0

BUCARAMANGA(config-if)#ip ospf message-digest-key 18 md5 java18

BUCARAMANGA(config-if)#ip ospf authentication message-digest

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#interface s0/0/0

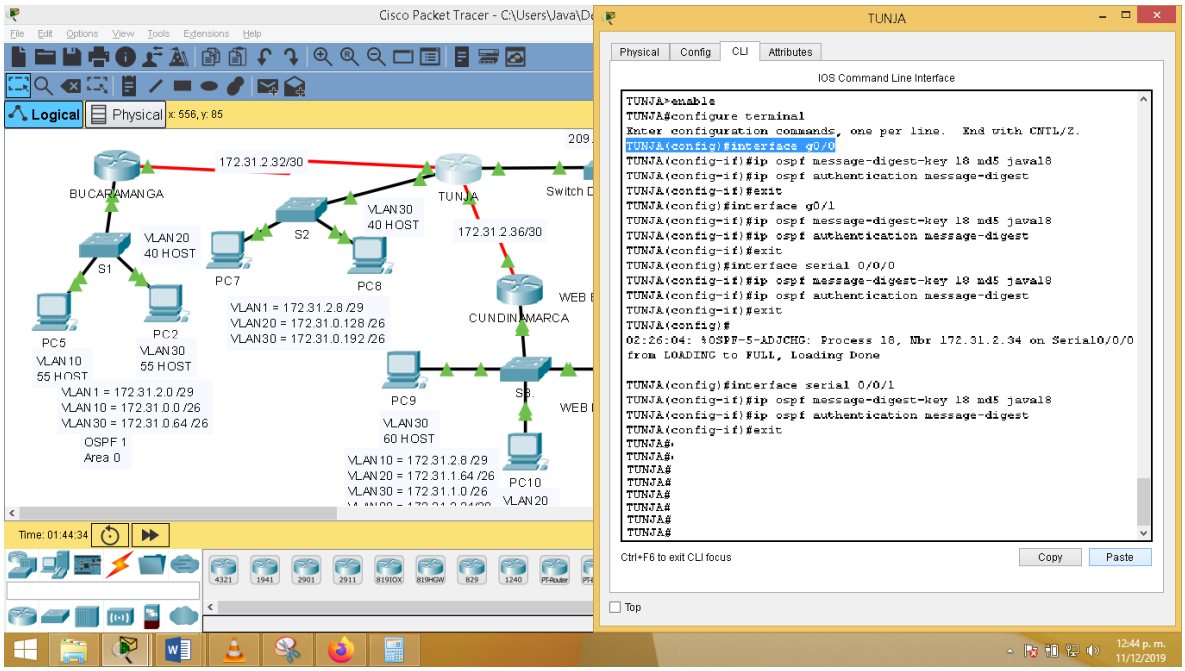
BUCARAMANGA(config-if)#ip ospf message-digest-key 18 md5 java18

BUCARAMANGA(config-if)#ip ospf authentication message-digest

BUCARAMANGA(config-if)#exit

Autenticación OSPF MD5, router Tunja.

Figura 88. Autenticación OSPF md5 router Tunja.



Fuente 97. prueba de habilidades prácticas, Autor: Javier Bulla.

Para crear autenticación en la subred, se ejecuta los siguientes comandos:

TUNJA(config)#interface g0/0

TUNJA(config-if)#ip ospf message-digest-key 18 md5 java18

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#exit

TUNJA(config)#interface g0/1

TUNJA(config-if)#ip ospf message-digest-key 18 md5 java18

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#exit

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#ip ospf message-digest-key 18 md5 java18

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#exit

TUNJA(config)#interface serial 0/0/1

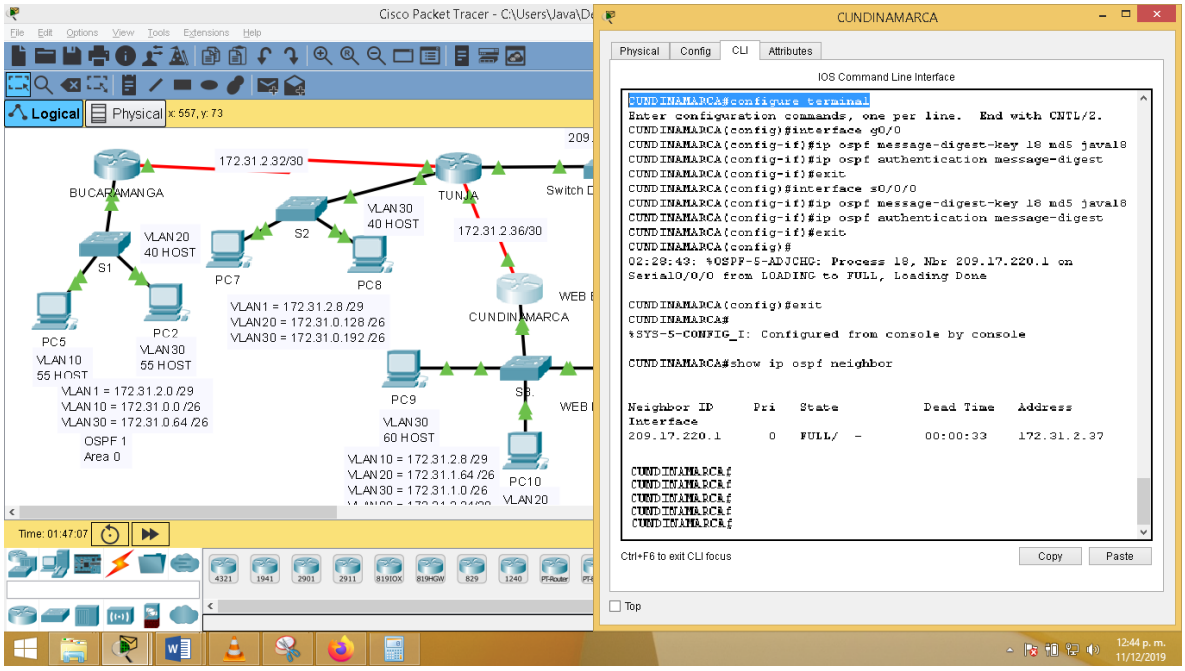
TUNJA(config-if)#ip ospf message-digest-key 18 md5 java18

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#exit

Autenticación OSPF MD5, router Tunja.

Figura 89. Autenticación OSPF md5 router Cundinamarca



Fuente 98. prueba de habilidades prácticas, Autor: Javier Bulla

Para crear autenticación en la subred, se ejecuta los siguientes comandos:

CUNDINAMARCA#configure terminal

CUNDINAMARCA(config)#interface g0/0

CUNDINAMARCA(config-if)#ip ospf message-digest-key 18 md5 java18

CUNDINAMARCA(config-if)#ip ospf authentication message-digest

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#interface s0/0/0

CUNDINAMARCA(config-if)#ip ospf message-digest-key 18 md5 java18

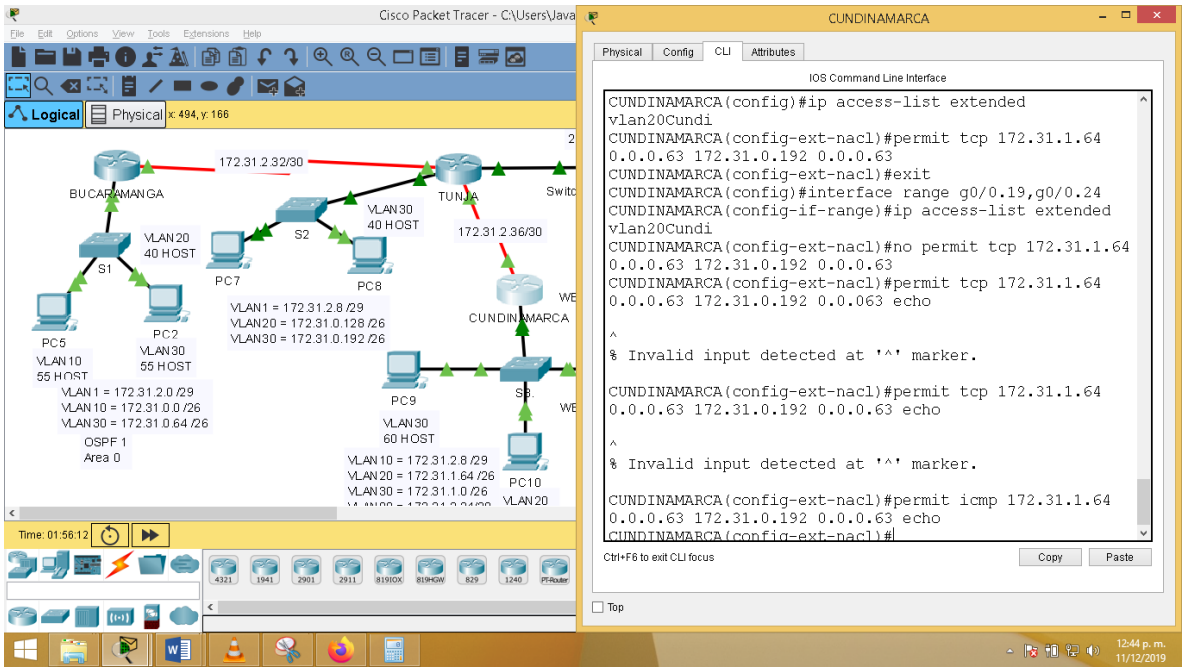
CUNDINAMARCA(config-if)#ip ospf authentication message-digest

CUNDINAMARCA(config-if)#exit

4.2. 8. Parte 8. Listas de control de acceso:

4.2.8.1 Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

Figura 90. Creando lista de acceso Extendida Router Cundinamarca



Fuente 99. prueba de habilidades prácticas, Autor: Javier Bulla

Para tal efecto se establece una lista de acceso extendida.

Para ello se ejecutan lo siguiente comandos.

comandos:

CUNDINAMARCA#configure terminal

CUNDINAMARCA(config)#ip access-list extended vlan20cundi

CUNDINAMARCA(config-ext-nacl)#permit icmp 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63 echo

CUNDINAMARCA(config-ext-nacl)#permit icmp 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63 echo

CUNDINAMARCA(config-ext-nacl)#permit icmp 172.31.1.64 0.0.0.63 172.31.2.8 0.0.0.7 echo

CUNDINAMARCA(config-ext-nacl)#exit

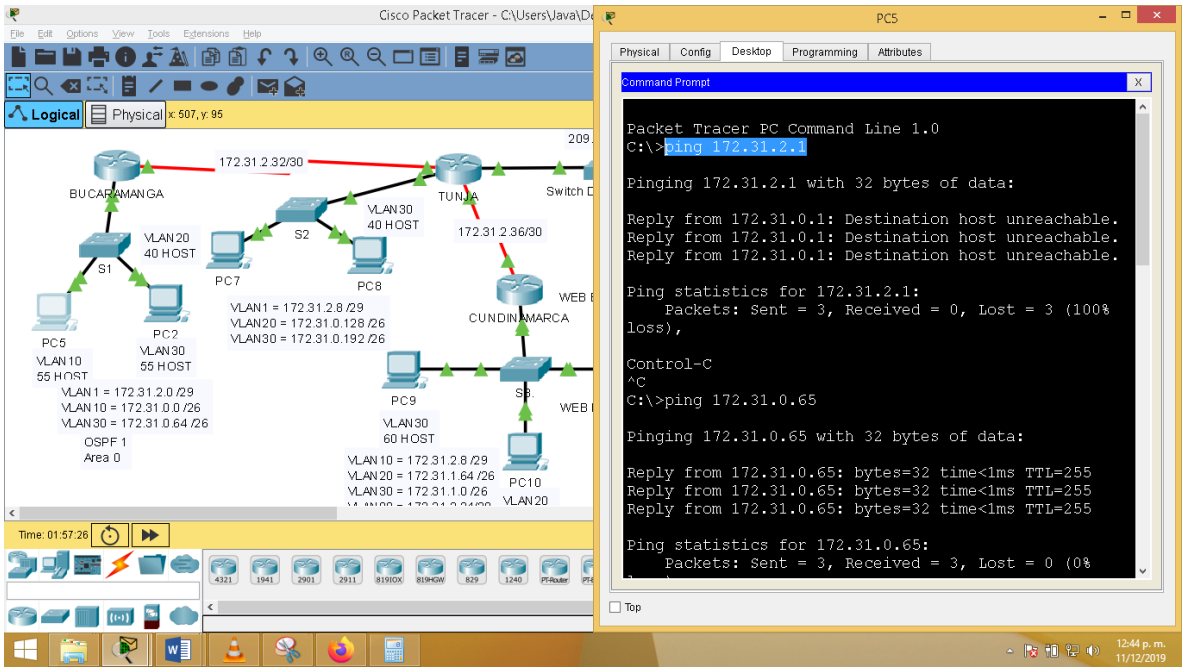
CUNDINAMARCA(config-ext-nacl)#exit

CUNDINAMARCA(config)#interface g0/0.24

CUNDINAMARCA(config-if-range)# ip access-group vlan20Cundi in

Verificando implementación.

Figura 91. Verificando implementación lista de acceso extendida router Cundinamarca



Fuente 100. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la implementación se ejecutarán los siguientes comandos:

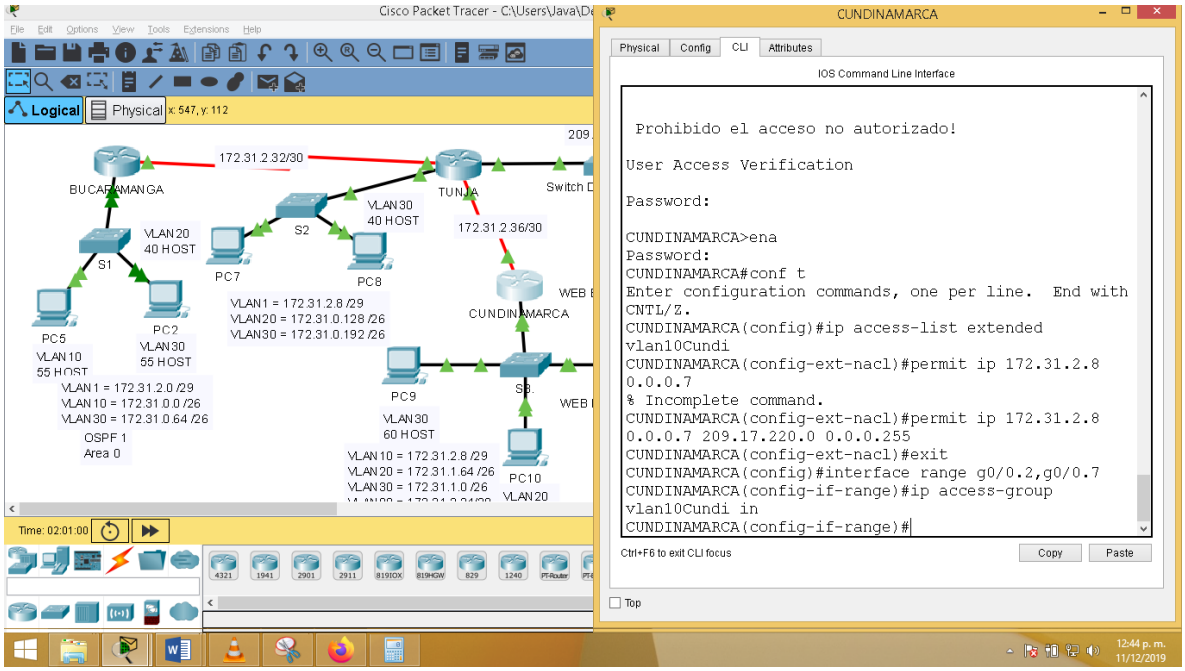
C:\>ping 209.17.220.1 → puerta de enlace a internet, resultado denegado.

C:\>ping 209.17.220.2 → puerta de enlace a servidor WEB externo, resultado denegado.

C:\>ping 172.31.0.130 → host subred Tunja, resultado exitoso.

4.2.8.2 Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

Figura 92. Verificando implementación lista de acceso extendida router Cundinamarca



Fuente 101. prueba de habilidades prácticas, Autor: Javier Bulla

Para tal efecto se establece una lista de acceso extendida.

Para ello se ejecutan lo siguiente comandos.

comandos:

CUNDINAMARCA#configure terminal

CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.2.8 0.0.0.7 209.17.220.0 0.0.0.255

CUNDINAMARCA(config-ext-nacl)#exit

CUNDINAMARCA(config)#

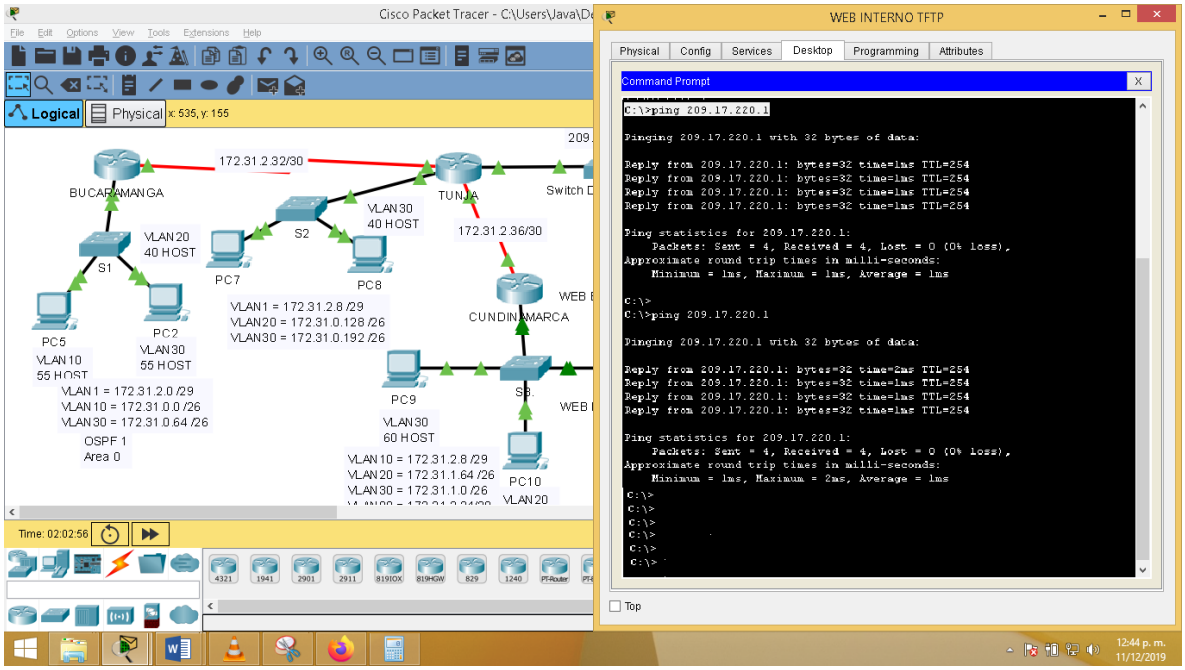
CUNDINAMARCA(config)#interface range g0/0.2,g0/0.7

CUNDINAMARCA(config-if-range)#ip access-group vlan10Cundi in

CUNDINAMARCA(config-if-range)#exit

Verificando implementación.

Figura 93. Verificando implementación de lista de acceso en vlan 10, router Cundinamarca



Fuente 102. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la implementación se ejecutarán los siguientes comandos:

C:\>ping 209.17.220.1 → puerta de enlace a internet, resultado Exitoso.

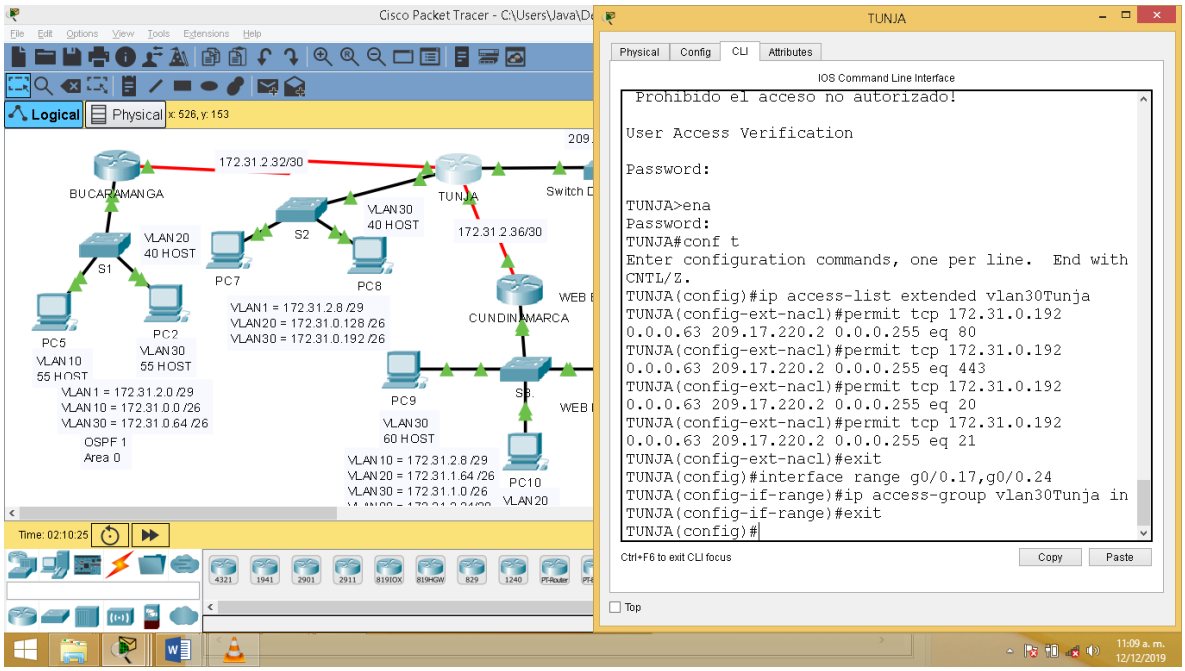
C:\>ping 209.17.220.2 → puerta de enlace a servidor WEB externo, resultado Exitoso.

C:\>ping 172.31.0.129 → host subred Tunja, resultado denegado.

C:\>ping 172.31.0.193 → host subred Tunja, resultado denegado.

4.2.8.3 Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

Figura 94. Configurando access lists vlan 30, en router Tunja



Fuente 103. prueba de habilidades prácticas, Autor: Javier Bulla

Para crear la lista de acceso, se ejecutan lo siguiente comandos:

TUNJA#configure terminal

TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 209.17.220.2 0.0.0.255 eq 80

TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 209.17.220.2 0.0.0.255 eq 443

TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 209.17.220.2 0.0.0.255 eq 20

TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 209.17.220.2 0.0.0.255 eq 21

TUNJA(config-ext-nacl)#exit

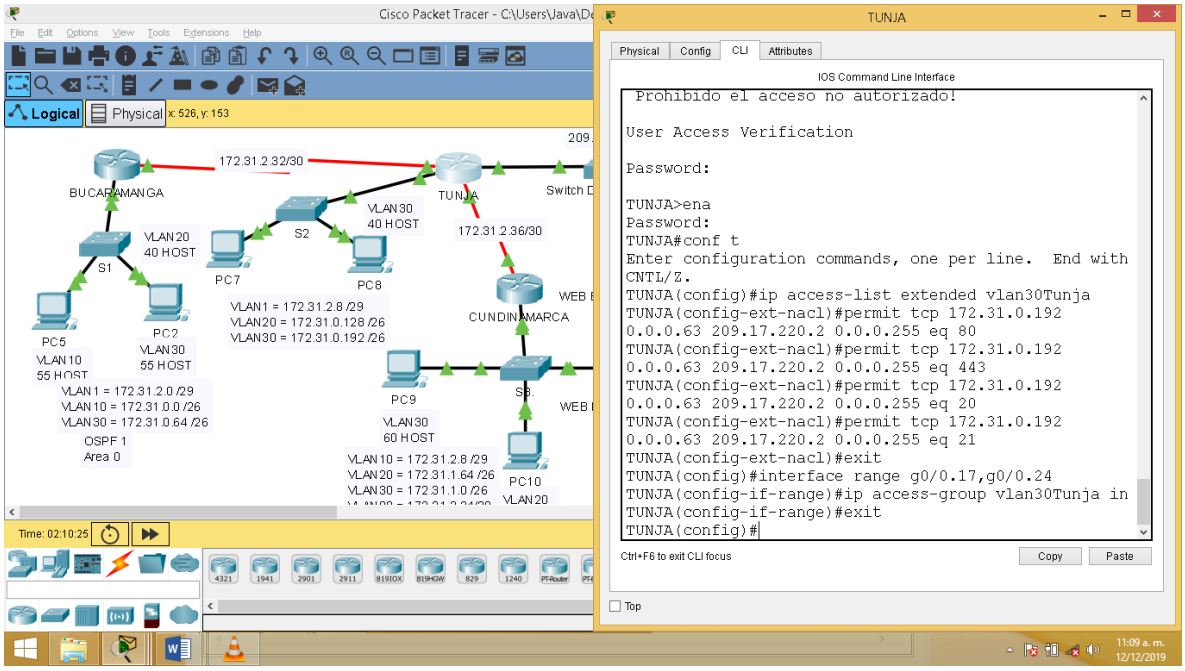
TUNJA(config)#

TUNJA(config)#interface range g0/0.17,g0/0.24

TUNJA(config-if-range)#ip access-group vlan30Tunja in

TUNJA(config-if-range)#exit

Verificando lista de acceso PC8 en vlan 30 subred Tunja



Fuente 104. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la implementación se ejecutarán los siguientes comandos:

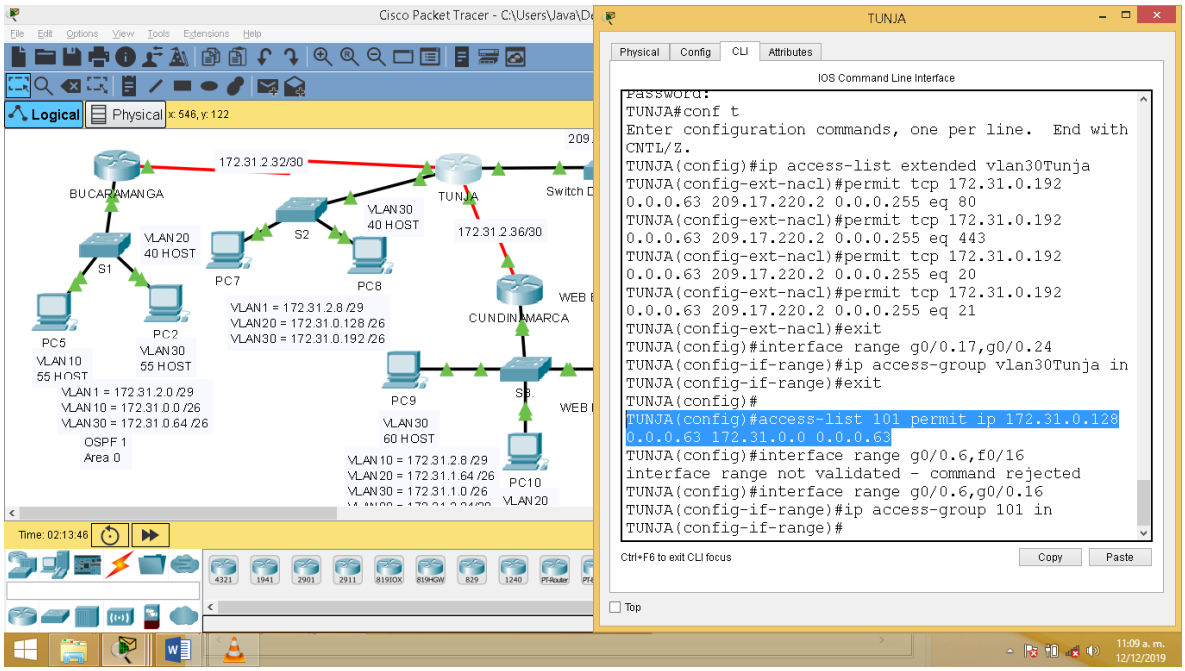
C:\>ping 209.17.220.1 → puerta de enlace a internet, resultado Exitoso.

C:\>ping 209.17.220.2 → puerta de enlace a servidor WEB externo, resultado Exitoso.

C:\>ping 172.31.0.129 → host subred Tunja, resultado denegado.

4.2.8.4 Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

Figura 95. Configurando access lists vlan 20, en router Tunja



Fuente 105. prueba de habilidades prácticas, Autor: Javier Bulla

Para crear la lista de acceso, se ejecutan lo siguiente comandos:

TUNJA#configure terminal

TUNJA(config)#access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

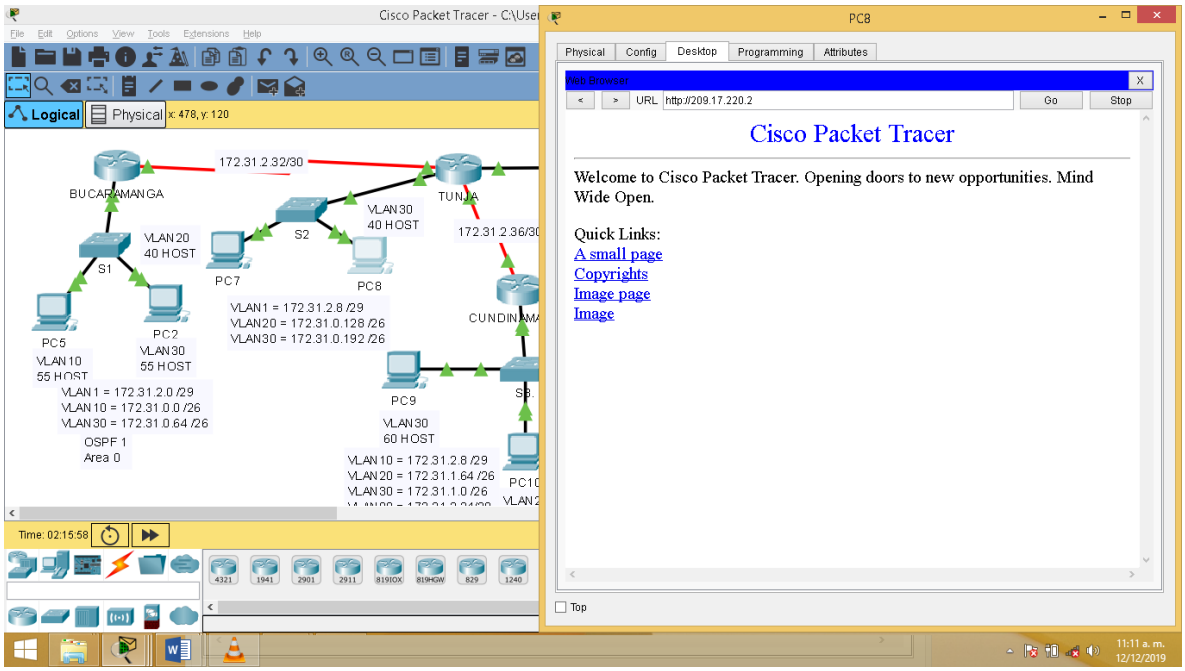
TUNJA(config)#interface range g0/0.6,g0/0.16

TUNJA(config-if-range)#ip access-group 101 in

TUNJA(config-if-range)#exit

Verificando protocolo http y https

Figura 96. Verificando ACL en vlan 10, router Tunja



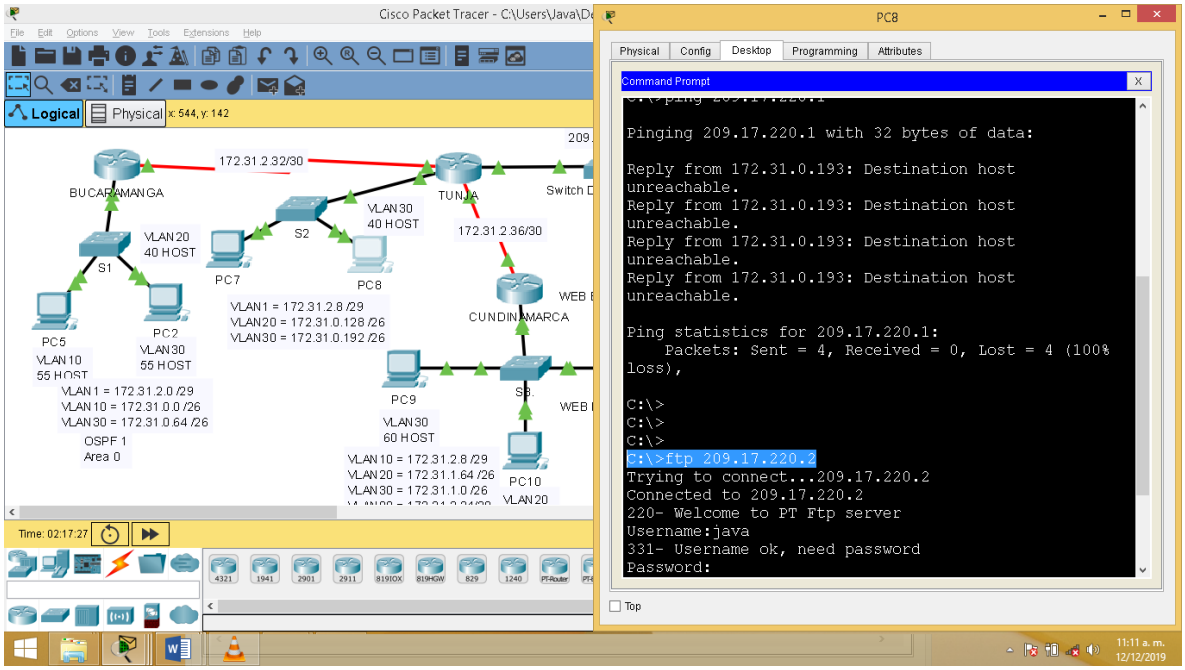
Fuente 106. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la implementación se abrirá el navegador del PC8 y en la barra de URL se ejecutará la dirección IP publica de Servidor externo:

C:\>ping 209.17.220.2 → puerta de enlace a servidor WEB externo, resultado exitoso protocolo WEB.

Verificando protocolo FTP

Figura 97. verificando acceso ftp, servidor externo publico



Fuente 107. prueba de habilidades prácticas, Autor: Javier Bulla

Para acceder al servidor ftp, externo público se digitan los siguientes comandos:

C:\>ftp 209.17.220.2

Username:java

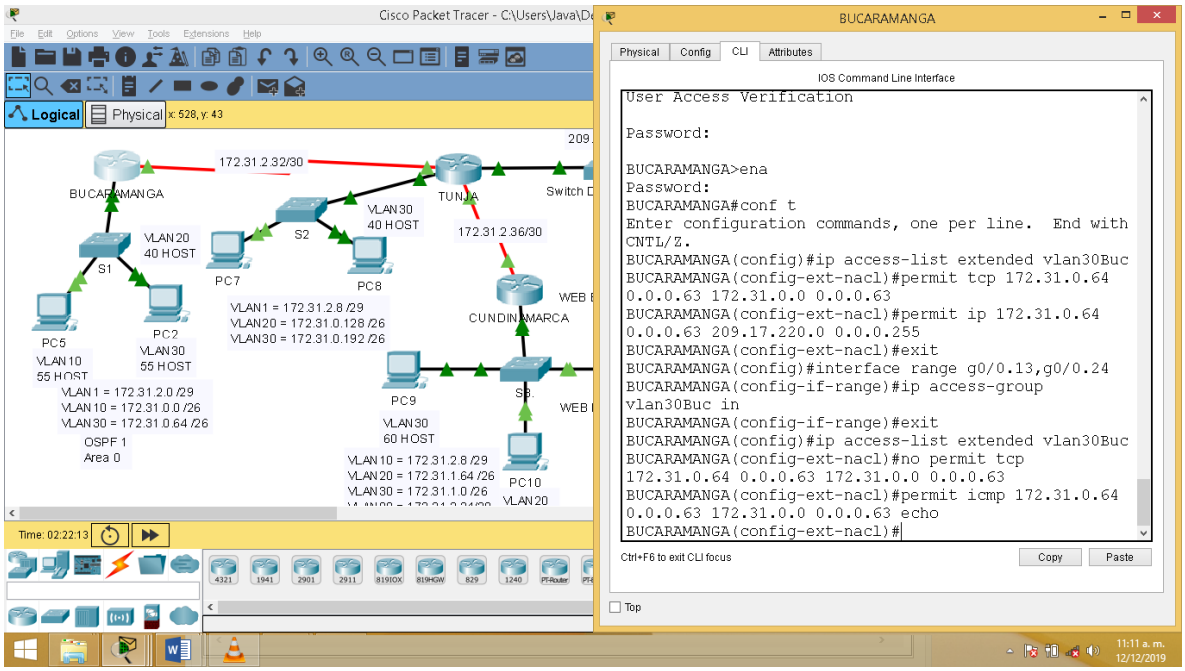
Password:

Si se digita correctamente se puede acceder al servidor FTP

ftp>

4.2.8.5 Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

Figura 98. Configurando lista de acceso, vlan 30 router Bucaramanga



Fuente 108. prueba de habilidades prácticas, Autor: Javier Bulla

Para crear la lista de acceso, se ejecutan lo siguiente comandos:

BUCARAMANGA(config-ext-nacl)#permit tcp 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63

BUCARAMANGA(config-ext-nacl)#permit icmp 172.31.0.64 0.0.0.63 209.17.220.0 0.0.0.255 echo

BUCARAMANGA(config-ext-nacl)#exit

BUCARAMANGA(config)#

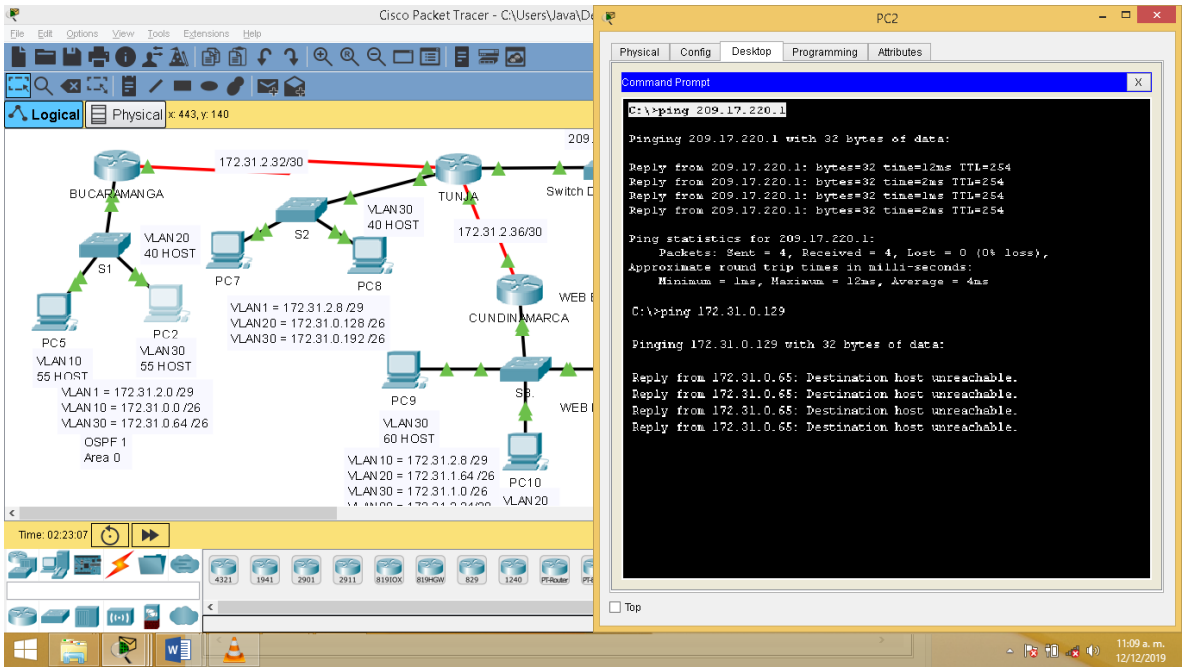
BUCARAMANGA(config)#interface range g0/0.13,g0/0.24

BUCARAMANGA(config-if-range)#ip access-group vlan30Buc in

BUCARAMANGA(config-if-range)#exit

Verificando funcionamiento de lista de acceso.

Figura 99. Verificando ACL en vlan 30, router Bucaramanga



Fuente 109. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la implementación se ejecutarán los siguientes comandos:

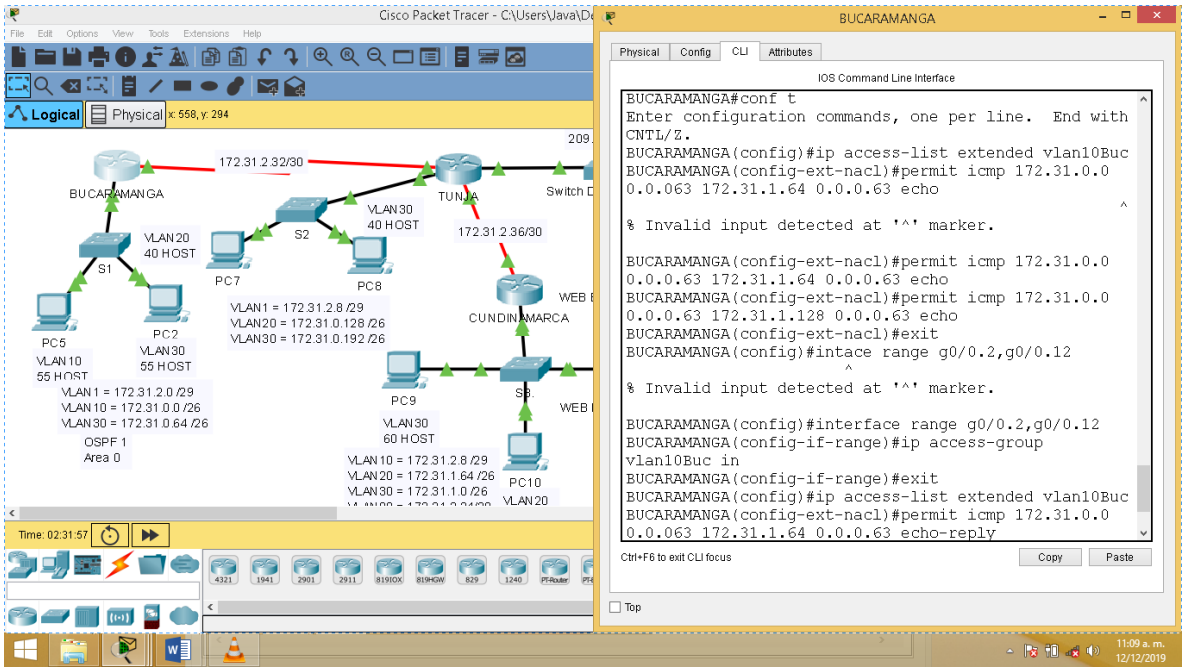
C:\> ping 209.17.220.1 puerta de enlace a internet, resultado Exitoso.

C:\> ping 172.31.0.2 puerta de enlace a PC5 vlan 10, Bucaramanga, resultado Exitoso.

C:\>ping 172.31.0.129 host externos, resultado Fallido.

4.2.8.6 Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN20), no internet.

Figura 100. Configurando lista de acceso, vlan 10 router Bucaramanga



Fuente 110. prueba de habilidades prácticas, Autor: Javier Bulla

Para crear la lista de acceso, se ejecutan lo siguiente comandos:

BUCARAMANGA(config)#ip access-list extended vlan10Buca

BUCARAMANGA(config-ext-nacl)#permit icmp 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63 echo

BUCARAMANGA(config-ext-nacl)#permit icmp 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63 echo

BUCARAMANGA(config-ext-nacl)#permit icmp 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63 echo-reply

BUCARAMANGA(config-ext-nacl)#exit

BUCARAMANGA(config)#

BUCARAMANGA(config)#interface range g0/0.2,g0/0.12

BUCARAMANGA(config-if-range)#ip access-group vlan10Buca in

BUCARAMANGA(config-if-range)#exit

BUCARAMANGA(config)#ip access-list extended vlan30Buca

BUCARAMANGA(config-ext-nacl)#no permit icmp 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63 echo

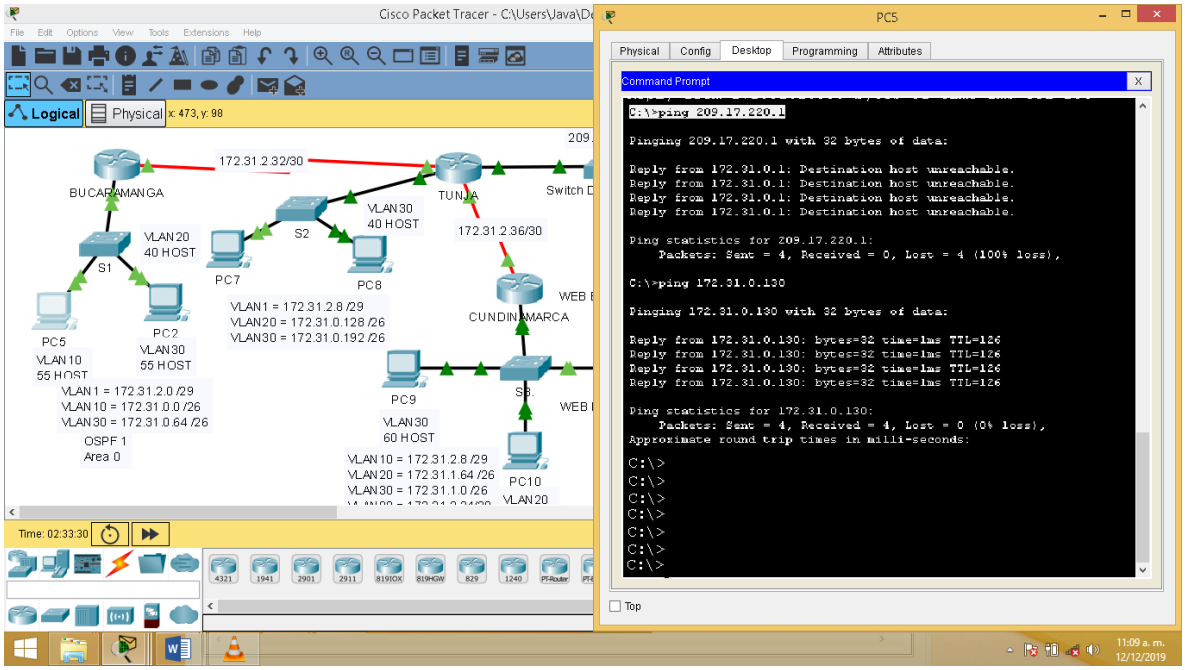
BUCARAMANGA(config-ext-nacl)#no permit icmp 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63 echo

BUCARAMANGA(config-ext-nacl)#permit icmp 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63 echo

BUCARAMANGA(config-ext-nacl)#permit icmp 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63 echo

Verificando implementación de lista de acceso.

Figura 101. Verificando ACL en vlan 10, router Bucaramanga



Fuente 111. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la implementación se ejecutarán los siguientes comandos:

C:\> ping 209.17.220.1 puerta de enlace a internet, resultado Fallido.

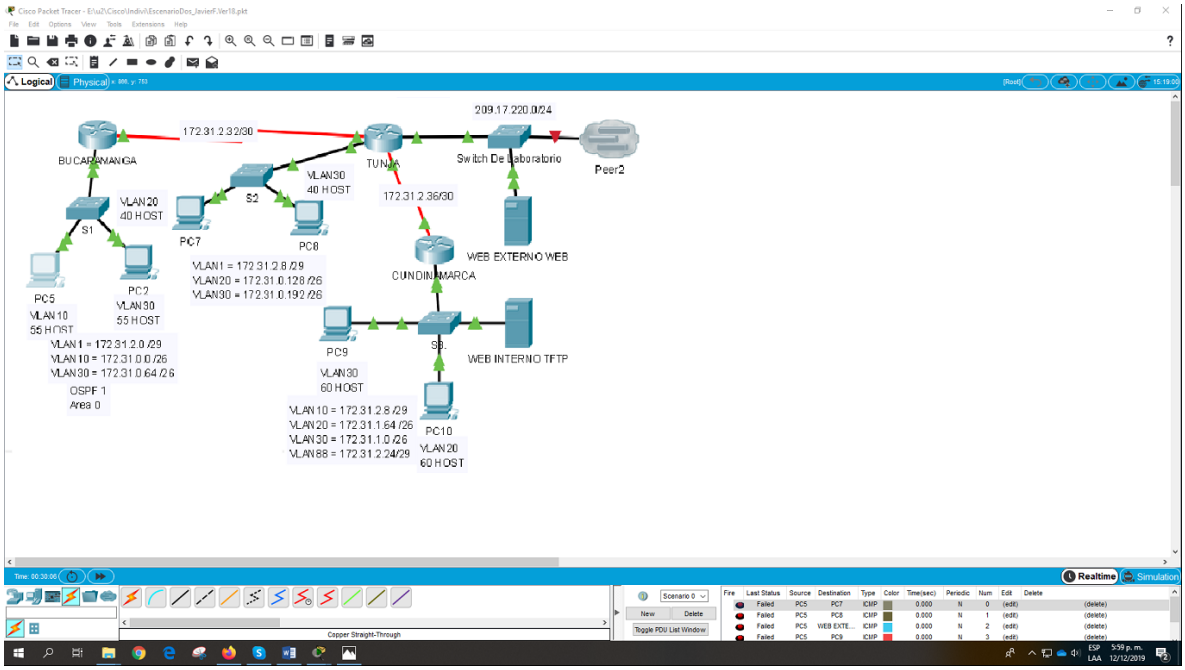
C:\> ping 172.31.0.130 host PC7 vlan 20, Tunja, resultado Exitoso.

C:\>ping 172.31.1.66 host PC7 vlan 20, Cundinamarca, resultado Exitoso.

4.2.8.7 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

Comprobando Conectividad con otras subredes y redes.

Figura 102. Verificando conectividad



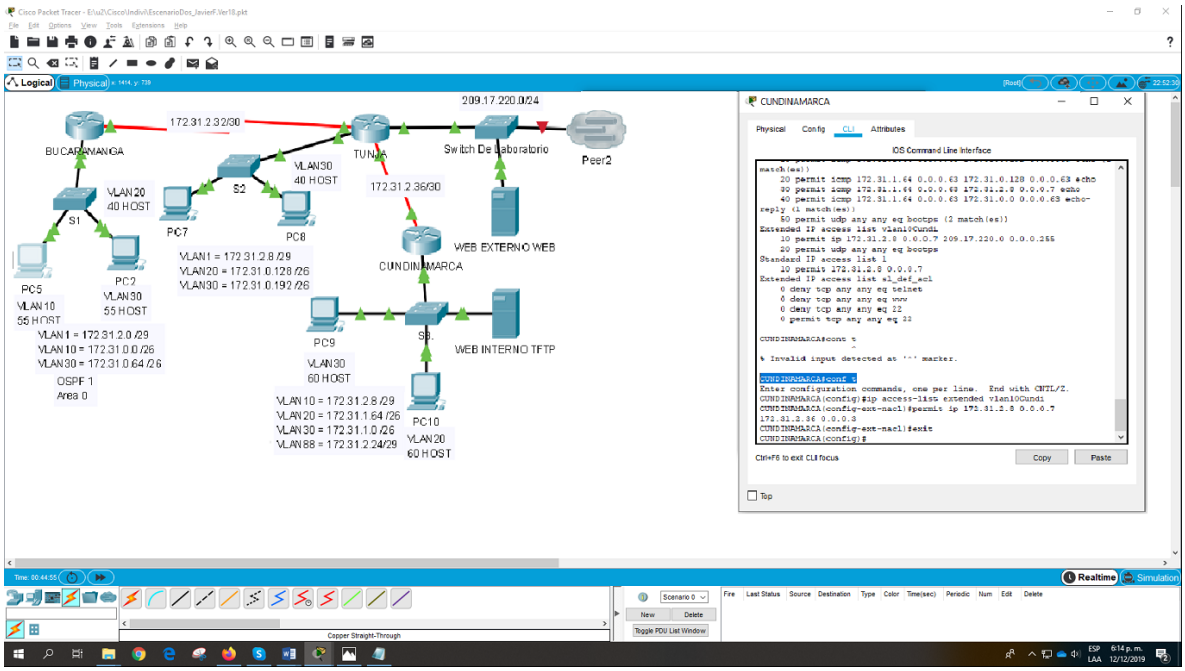
Fuente 112. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar la conectividad con otras redes y subredes, se ejecuta el comando PING

4.2.8.8 Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los router se internet

Configurando acceso por telnet en router Cundinamarca.

Figura 103. Configurando telnet, router Cundinamarca



Fuente 113. prueba de habilidades prácticas, Autor: Javier Bulla a

Para configurar el acceso por telnet, al router Cundinamarca, se ejecutan los siguientes comandos:

CUNDINAMARCA(config)#access-list 1 permit 172.31.2.8 0.0.0.7

CUNDINAMARCA(config)#line vty 0 15

CUNDINAMARCA(config-line)#access-class 1 in

CUNDINAMARCA(config-line)#exit

CUNDINAMARCA(config)#ip access-list extended vlan10Cundi

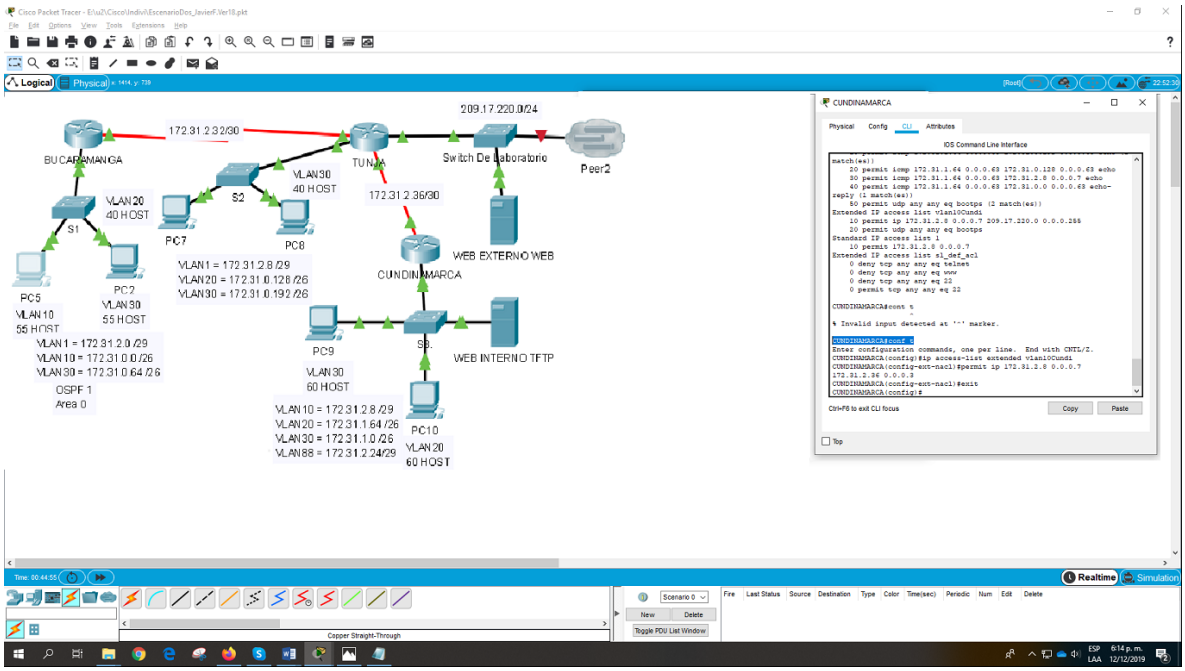
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.2.8 0.0.0.7 172.31.2.36 0.0.0.3

CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.2.8 0.0.0.7 172.31.2.32 0.0.0.3

CUNDINAMARCA(config-ext-nacl)#exit

Verificando implementación de acceso telnet

Figura 104. Verificando acceso telnet, servidor TFTP



Fuente 114. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar el acceso telnet, del servidor al router Cundinamarca, se ejecuta el siguiente comando:

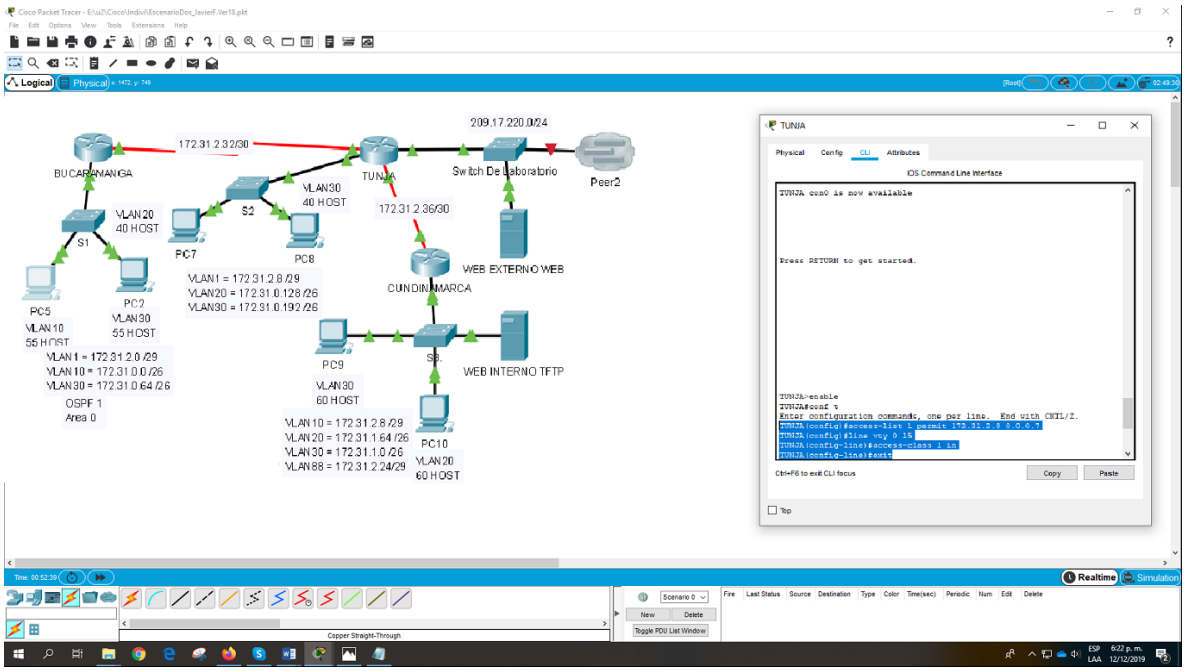
C:\>telnet 172.31.2.38

Password:

CUNDINAMARCA>exit

Configurando acceso por telnet en router Tunja.

Figura 105. Configurando telnet, router Tunja



Fuente 115. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el acceso por telnet, al router Cundinamarca, se ejecutan los siguientes comandos:

TUNJA(config)#access-list 1 permit 172.31.2.8 0.0.0.7

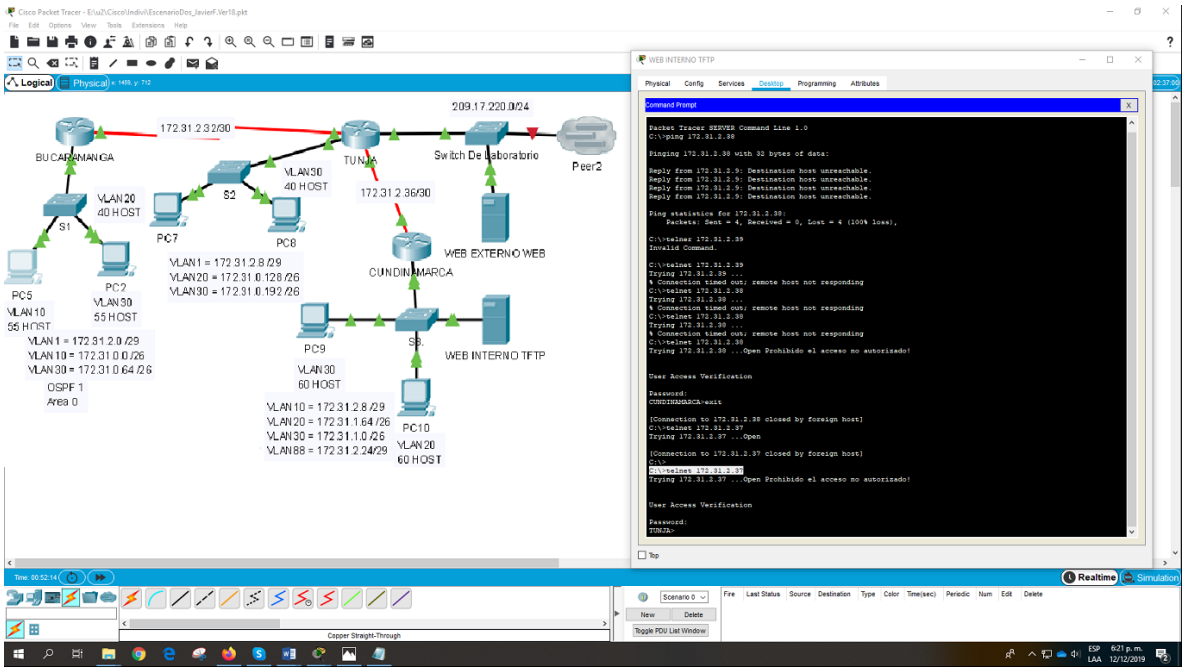
TUNJA(config)#line vty 0 15

TUNJA(config-line)#access-class 1 in

TUNJA(config-line)#exit

Verificando implementación.

Figura 106. Verificando acceso telnet, servidor TFTP



Fuente 116. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar el acceso telnet, del servidor al router Cundinamarca, se ejecuta el siguiente comando:

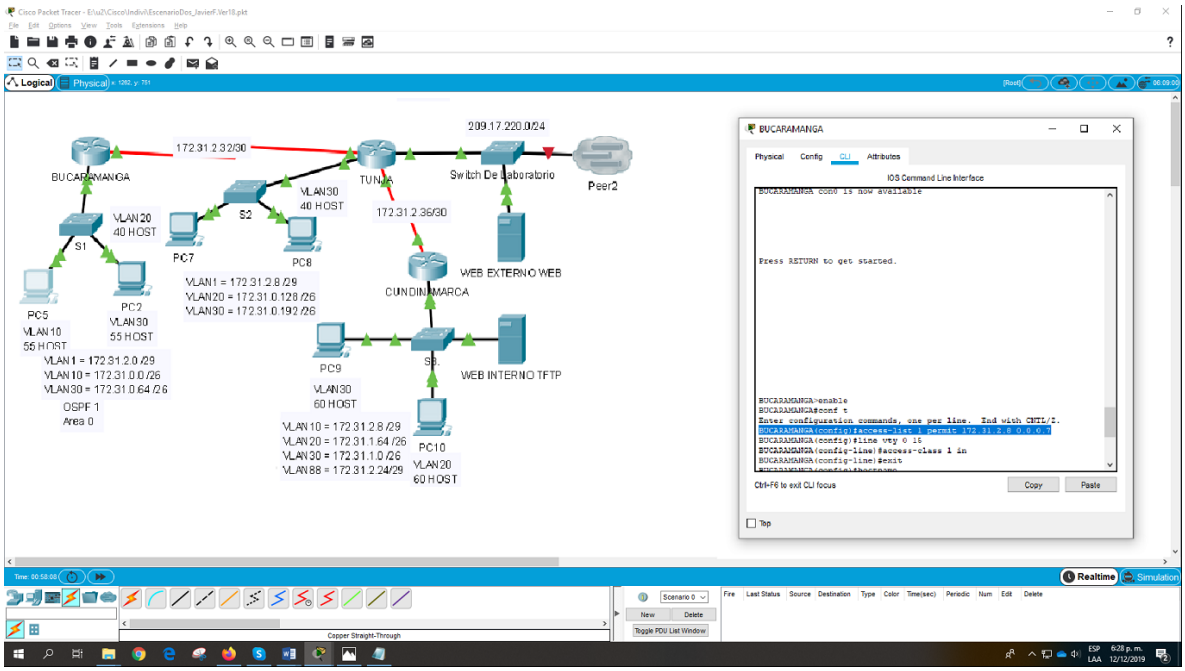
C:\>telnet 172.31.2.37

Password:

TUNJA>exit

Configurando acceso por telnet en router Bucaramanga.

Figura 107. Configurando telnet, router Bucaramanga



Fuente 117. prueba de habilidades prácticas, Autor: Javier Bulla

Para configurar el acceso por telnet, al router Cundinamarca, se ejecutan los siguientes comandos:

BUCARAMANGA(config)#access-list 1 permit 172.31.2.8 0.0.0.7

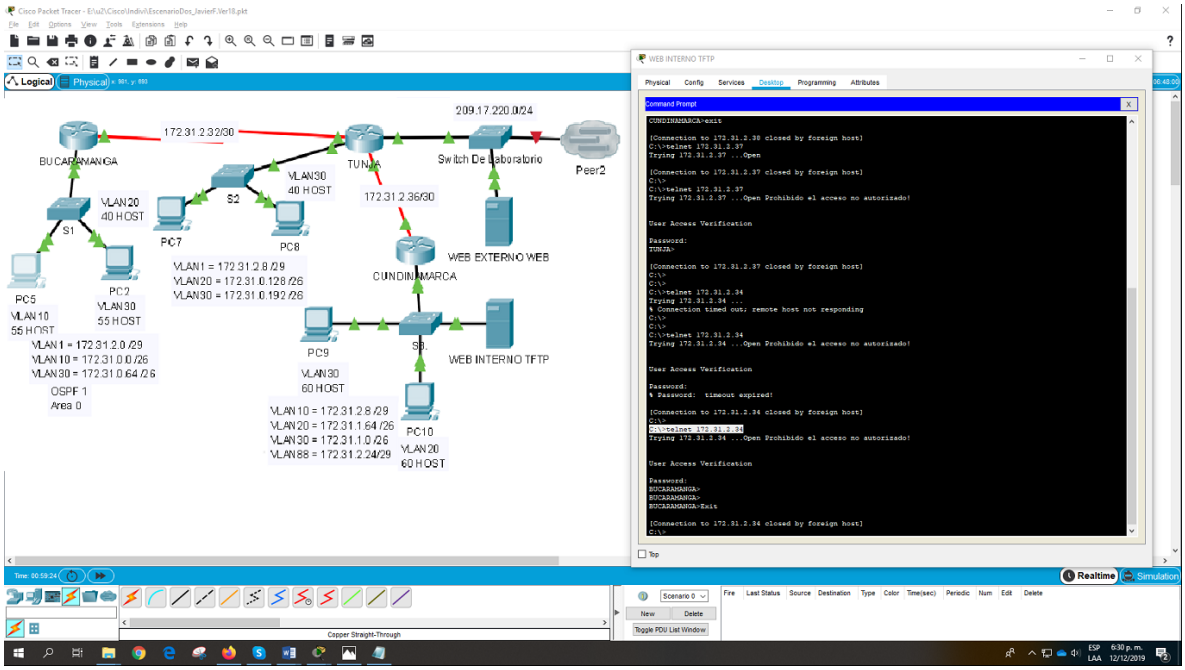
BUCARAMANGA (config)#line vty 0 15

BUCARAMANGA (config-line)#access-class 1 in

BUCARAMANGA (config-line)#exit

Verificando implementación.

Figura 108. Verificando acceso telnet, servidor TFTP



Fuente 118. prueba de habilidades prácticas, Autor: Javier Bulla

Para verificar el acceso telnet, del servidor al router Cundinamarca, se ejecuta el siguiente comando:

C:\>telnet 172.31.2.37

Password:

BUCARAMANGA >exit

En conclusión hay conexión remota TFTP, lo cual permite guardar los archivos de configuración de los dispositivos capa tres, esto es bien conocido como respaldos.

4.2.9. Parte 9. Nota

4.2.9.1 NOTA

Para acceder a la simulación dirigirse a anexos, donde se encontrará el link, de acceso.

5. CONCLUSIONES

En conclusión, la prueba de habilidades practicas dispuesta en el diplomado, PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), permitieron poner en pericia los conceptos en los módulos que se abordaron a lo largo del curso, de tal manera que se llevaron a cabo soluciones para redes según se especificaban, tales como:

Listas de acceso, permite restringir la entrada o salidas de paquetes, de una interfaz de router, lo cual permite estructurar redes de forma compleja y seguras evitando su vulnerabilidad.

Las listas de acceso estándar permiten la restricción de redes o host, pero son genéricas, cabe anotar que son más simples en situaciones que no ameriten una restricción estricta, en el escenario uno, se implementa una lista de acceso simple para permitir el acceso por protocolo remoto telnet.

Las listas de acceso extendidas, son más complejas, pero requieren una habilidad en el manejo de protocolos y puertos, ya que principalmente se estructuran bajo dichas métricas, de igual manera estas permiten diseñar redes y subredes más seguras, la correcta implementación de las misma optimiza el tráfico de la red, ya que no todos los hosts de una red requieren los mismos servicios, ni se le pueden conceder a todos, acceso libre.

Para finalizar el diseño de una red, como se evidencio en el escenario uno y dos, requirieron la aplicación de todos los conceptos vistos en el diplomado de cisco CNNA, tales como subneteo, de red, vlans, listas de acceso, protocolos de red, configuración básica de routers, de switch, acceso remoto telnet y ssh, solo por nombrar unos.

6. RECOMENDACIONES

Se recomienda, para más comprensión el análisis de los comandos de entrada que se describen en cada proceso, de tal manera que se entienda el proceso llevado a cabo, de igual manera las ilustraciones, también son una fuente de información que permite describir la implementación en cada transcurso de fase de cada escenario.

Para finalizar se dispone de la simulación en un link de drive la cual se implementó, para el desarrollo de este documento Prueba de Habilidades Practicas.

7. BIBLIOGRAFIA

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

8. ANEXOS

Para descargar la simulación, acceder al siguiente LINK.

https://drive.google.com/drive/folders/1zHAaifX-UgKVPokpwkAZhF5aXamuf8_3?usp=sharing